Smart 108/116 IP

User Guide

www.minicom.com

International HQ

Jerusalem, Israel

Tel: + 972 2 535 9666

minicom@minicom.com

North American HQ

Linden, NJ, USA

Tel: + 1 908 486 2100

info.usa@minicom.com

Technical Support – support@minicom.com

SC_5UM21166 V2.0 4/11

Legal Notice

About this Document

This document provides installation and operation instructions for the Smart 108/116 IP system, produced by Minicom Advanced Systems Limited. It is intended for system administrators and network managers.

Chapters and Their Contents

1	**Introduction**	Provides an introduction to the document, Smart 108/116 IP product overview, features and benefits of Smart 108/116 IP, client computer operating system requirements, technical precautions, trademarks, and terminology used in the document. It also describes how to safely handle the device, provide feedback on the user guide, and WEEE Information for Minicom Customers and Recyclers.	Pg. 12
2	**Installation**	Lists Smart 108/116 IP system components, describes the functionalities of the Smart 108/116 IP elements, and provides instructions for rack mounting the unit and connecting the system.	Pg. 14
3	**Configuring the Network**	Provides instructions for logging into the Web configuration interface, configuring the device ID, IP address, and Centralized Management settings, enabling and configuring SNMP, adding, editing, removing, and blocking system Users, configuring the KVM switch, and security settings. It also provides instructions for installing an SSL certificate, upgrading firmware, restoring factory settings, and saving changes and logging out.	Pg. 25
4	**Conducting a Remote Session**	Describes how to start a remote session, set the session profile, full screen mode, view system information, adjust video settings, manage keyboard sequences, synchronize mouse pointers, switch to a different server or device, and disconnect the remote session.	Pg. 41
5	**Troubleshooting – Safe Mode**	Describes how to enter Safe mode, restore factory defaults, and restore device firmware.	Pg. 62
6	**Operating the Smart 108/116 IP Switching System Locally**	Describes how to operate Smart 108/116 IP using the keyboard hotkeys and the OSD, how to upgrade the firmware, and how to troubleshoot problems that occur when updating the software.	Pg. 66
7	**Technical Specifications**	Lists and describes Smart 108/116 IP specifications.	Pg. 87

8	**Video Resolution and Refresh Rates**	Lists video resolutions and refresh rates.	Pg. 87
9	**SNMP Events Table**	Lists recorded SNMP events.	Pg. 90

Style Conventions

Convention	Used for
Verdana	Regular text.
Arial Bold	Names of menus, commands, buttons, and other elements of the user interface.
Arial Italics	Special terms, the first time they appear.
`Monospace`	Text entered by the user.
	**Notes,** which offer an additional explanation or a hint on how to overcome a common problem.
	**Warnings**, which indicate potentially damaging user operations and explain how to avoid them.

Table of Contents

TABLE OF FIGURES X

1 INTRODUCTION 12

1.1 PRODUCT OVERVIEW 12

1.1.1 Features and Benefits 12

1.2 TERMINOLOGY 13

1.3 COMPATIBILITY 13

1.4 CLIENT COMPUTER OPERATING SYSTEM 13

1.5 TECHNICAL PRECAUTIONS 13

1.6 SAFETY 14

1.7 USER GUIDE FEEDBACK 14

1.8 TRADEMARKS 14

1.9 WEEE COMPLIANCE 14

2 INSTALLATION 16

2.1 OVERVIEW 16

2.2 SYSTEM COMPONENTS 16

2.2.1 The Smart 108/116 IP Unit 16

2.3 PRE-INSTALLATION GUIDELINES 18

2.4 RACK MOUNTING THE SMART 108/116 IP UNIT 18

2.4.1 Rack Mounting Safety Considerations 18

2.4.2 Mounting the Unit 19

2.5 CONNECTING THE SYSTEM 20

2.6 CONNECTING TO THE SERVERS 20

2.6.1 Connecting a RICC/ROC PS/2 21

2.6.2 Connecting a RICC/ROC USB 22

2.6.3 Connecting a RICC SUN 23

2.7 CONNECTING TO THE NETWORK 24

2.8 CONNECTING THE CAT5 CABLES 24
2.9 CONNECTING THE KVM CONSOLE 24
2.10 CONNECTING THE POWER SUPPLY 24
3 CONFIGURING THE NETWORK 25
3.1 BOOT-UP PROCESS 25
Assigning Static IP Addresses for a Number of Units 26
3.2 LOGGING ONTO THE WEB CONFIGURATION INTERFACE 27
3.2.1 Web Configuration Interface Tabs 28
3.2.2 Web Configuration Toolbar Buttons 29
3.3 CONFIGURING THE NETWORK SETTINGS 29
3.3.1 Configuring Device ID Settings 29
3.3.2 Configuring the Device IP Address 30
3.3.3 Configuring Centralized Management Settings 30
3.4 CONFIGURING NETWORK SNMP SETTINGS 31
3.5 CONFIGURING USER SETTINGS 32
3.5.1 Adding a User 32
3.5.2 Deleting User(s) 33
3.5.3 Blocking a User 34
3.5.4 Editing User Information 34
3.6 CONFIGURING THE KVM SWITCH 35
3.7 CONFIGURING THE SECURITY SETTINGS 36
3.8 PERFORMING ADDITIONAL CONFIGURATION OPERATIONS 38
3.8.1 Installing an SSL Certificate 38
3.8.2 Upgrading Firmware 39
3.8.3 Restoring Factory Settings 40
3.9 RELOADING A PAGE 41
3.10 SAVING CHANGES AND LOGGING OUT 41
4 CONDUCTING A REMOTE SESSION 43
4.1 STARTING A REMOTE SESSION 43
4.1.1 Remote Session Toolbar Buttons 45
4.2 SHARING A REMOTE SESSION 46

4.2.1 Exclusive Session 46
4.3 Displaying the Toolbar 46
4.4 Setting the Session Profile 46
4.4.1 Full Screen Mode 47
4.5 Verifying Remote Presence Solutions Information 48
4.6 Changing the Video Performance Settings 49
4.7 Adjusting the Video 50
4.7.1 Refreshing the Video Image 50
4.7.2 Automatically Adjusting the Video Image 51
4.7.3 Manually Adjusting Video Settings 51
4.8 Managing Keyboard Sequences 53
4.8.1 Adding A Keyboard Sequence 53
4.8.2 Recording a New Custom Key 55
4.8.3 Editing a Key Sequence 56
4.8.4 Deleting Key Sequence(s) 56
4.9 Synchronizing Mouse Pointers 56
4.9.1 Manually Synchronizing the Mouse 57
The USB Option 58
Advanced Mouse Emulation 59
4.9.2 Aligning the Mouse Pointers 60
4.9.3 Calibrating Mouse Pointers 60
4.10 Switching to a Different Server 60
4.11 Disconnecting the Remote Session 61
5 TROUBLESHOOTING – SAFE MODE 62
5.1 Entering Safe Mode 62
5.2 Restoring Factory Defaults 64
5.3 Restoring the Device Firmware 64
6 OPERATING THE SMART 108/116 IP SWITCHING SYSTEM LOCALLY .. 66
6.1 Using the Keyboard Hotkeys 66
6.2 Using the OSD 66
6.2.1 Navigating the OSD 67

6.2.2 Selecting a Computer 67
6.2.3 Configuring the OSD Settings 68
6.2.4 Configuring the General Settings 68
Configuring Security Settings 69
Changing the OSD Hotkey 70
Activating Autoskip 70
Serial Port 71
Changing the Keyboard Language 71
Editing the Switch Name 71
Restoring OSD to Factory Defaults (F7) 71
6.2.5 Configuring the Ports Settings 71
Editing the Computer Name 72
Modifying the Keyboard Setting 72
6.2.6 Configuring the Time Settings 73
Setting the Scan, Label, and Timeout Period 73
6.2.7 Configuring the Users Settings 74
6.2.8 Configuring the Security Settings 75
6.2.9 OSD Functions (F1) 75
Scanning Computers (F4) 76
Tuning (F5) 77
Moving the Label (F6) 77
Inputting and Updating DDC Information (F10) 77
6.3 UPGRADING THE SMART 108/116 IP FIRMWARE 78
6.3.1 Downloading Update Software and Latest Firmware 78
6.3.2 Update Software System Requirements 79
6.3.3 Connecting the Smart 108/116 IP System 79
6.3.4 Connecting the RS232 Download Cable 79
6.3.5 Installing the Software 80
6.3.6 Starting and Configuring the Update Software 80
6.3.7 Verifying the Version Numbers 82
Smart 108/116 IP Switch Version 82
RICC/ROC Version 83
6.3.8 Obtaining New Firmware 83
Updating the Firmware 83
Manually Updating the RICC/ROCs 85
6.3.9 Restoring Factory Settings 85

6.4 TROUBLESHOOTING – UPDATE SOFTWARE 85
6.4.1 Communication Error Message 85
6.4.2 Electricity Failure..... 86
7 TECHNICAL SPECIFICATIONS 87
8 VIDEO RESOLUTION AND REFRESH RATES 89
9 SNMP EVENTS TABLE 90

Table of Figures

Figure 1 – Smart 108/116 IP Unit Front Panel 16
Figure 2 – Smart 116 IP Unit Rear Panel 17
Figure 3 – Bracket Positions 19
Figure 4 – Bracket Connected for Rear Facing 19
Figure 5 – Smart 108/116 IP System Overview 20
Figure 6 – ROC PS/2 21
Figure 7 – ROC USB 21
Figure 8 – RICC PS/2 Connections 22
Figure 9 – RICC USB 23
Figure 10 – RICC SUN 23
Figure 11 – Boot-Up Process 26
Figure 12 – Web Page 27
Figure 13 – Logon Page 27
Figure 14 – Network Configuration – Device Tab 28
Figure 15 – SNMP Settings 31
Figure 16 – Users Page 32
Figure 17 – Add User Page 33
Figure 18 – Delete User Confirmation 34
Figure 19 – Edit User Page 35
Figure 20 – KVM Switch Configuration Page for Smart 116 IP 36
Figure 21 – Security Page 37
Figure 22 – SSL Certificate Page 38
Figure 23 – Device Version Upgrade Page 39
Figure 24 – Reboot Confirmation Page 39
Figure 25 – Restore Factory Settings Page 40
Figure 26 – Device Reboot Confirmation Message 41
Figure 27 – Save Succeeded Message 42
Figure 28 – Device Rebooting Progress Box 42
Figure 29 – Logon Page after Rebooting 42
Figure 30 – Logon Page 44
Figure 31 – Remote Session Page 44
Figure 32 – Shared Remote Session 46
Figure 33 – Session Profile Dialog Box 47
Figure 34 – Remote Presence Solutions Information 48
Figure 35 – Performance Settings 50
Figure 36 – Video Adjust Progress 51
Figure 37 – Manual Video Adjustments Controls 52
Figure 38 – Special Key Manager 54
Figure 39 – Add a Predefined Key Dialog Box 54

Figure 40 – Record Macro Box 55
Figure 41 – Delete Key(s) Confirmation Box 56
Figure 42 – Relative Mouse Settings 57
Figure 43 – Windows 7 Mouse Properties 58
Figure 44 – Mouse Emulation Box 59
Figure 45 – Safe Mode Procedure 62
Figure 46 – Login Page 63
Figure 47 – Safe Mode Menu 63
Figure 48 – Warning 64
Figure 49 – Additional Warning 64
Figure 50 – Reboot 64
Figure 51 – Upgrade Succeeded 65
Figure 52 – OSD Main Window 67
Figure 53 – OSD Settings Window 68
Figure 54 – General Settings Window 69
Figure 55 – Ports Settings Window 72
Figure 56 – Time Settings Window 73
Figure 57 – Users Settings Window 74
Figure 58 – Security Settings Window 75
Figure 59 – The OSD HELP Window 76
Figure 60 – RS232 Cable 80
Figure 61 – Smart 108/116 IP Switch Update Window 81
Figure 62 – Communication Port Dialog box 82
Figure 63 – Firmware Version Report 82
Figure 64 – Hardware Version Report 83
Figure 65 – Open Dialog Box 84

1 Introduction

Congratulations on adding Smart 108/116 IP to your remote access tools.

This document provides installation and operation instructions for Minicom's Smart 108/116 IP. It is intended for system administrators and network managers, and assumes that readers have a general understanding of networks, hardware, and software.

Chapter 3 and Chapter 4 of this guide describe how to configure and operate the Smart 108/116 IP system remotely over IP. Chapter 6 explains how to operate the Smart 108/116 IP switching system locally through the On Screen Display (OSD).

1.1 Product Overview

The Smart 108/116 IP system extends your KVM (keyboard, video, and mouse) from any computer or server over TCP/IP via LAN, WAN, or Internet connection. This enables you to control, monitor, and manage up to 8/16 remote servers from wherever you are, inside or outside the organization. Smart 108/116 IP is a cost-effective hardware solution, for secure, remote KVM access and control of 8/16 computers/servers from the BIOS level – independent of the OS. One local analog or one remote digital IP user can access and control 8/16 multi-platform (PS/2, SUN, or USB) servers.

Smart 108/116 IP is based on Minicom's innovative ROC technology, in which each computer/server is directly connected to the switch via ROC dongles using only a standard CAT5 cable at a distance of up to 30 m / 100 ft in a star configuration. No external power is needed at the remote ROC.

The Smart 108 IP and Smart 116 IP are functionally the same. The Smart 108 IP has eight Server ports; the Smart 116 IP has 16 Server ports.

1.1.1 Features and Benefits

Smart 108/116 IP has the following features and benefits:

- **BIOS level control** to any server's brand and model, regardless of the server condition and network connectivity. Covers the entire spectrum of crash scenarios.
- **Compatible** with all major operating systems.
- **Web-based control** – Browser based control of a target server from any location, via a secured standard IP connection.

- **Multi-user share mode** – Allows up to five simultaneous users to share a remote session.
- **Security** – Supports the highest security standards for encryption (256-bit AES and HTTPS) and authentication for remote user and advanced OSD management, with multi-layer security for the local user.
- **Centralized Management** – Can be controlled by Minicom's AccessIT/KVM.net systems for centralized over-IP management of distributed data center locations.

1.2 Terminology

The following table describes terms used in this guide.

Term	Definition
Target server	The computer/server that is accessed remotely via Smart 108/116 IP
Client computer	The PC running a remote Smart 108/116 IP session
Remote session	The process of accessing and controlling target servers connected to Smart 108/116 IP from a user workstation

1.3 Compatibility

Smart 108/116 IP is compatible with:

- PS/2, SUN, and USB computers/servers
- VGA, SVGA, and XGA monitors
- Windows, Linux, UNIX, and other major operating systems

1.4 Client Computer Operating System

The client computer operating system must be one of the following:

- Windows 2000 or later, with Firefox 3 or Internet Explorer 32-bit 7.0 or later version
- Linux with Firefox 3; 128-bit encryption support is required

1.5 Technical Precautions

This equipment generates radio frequency energy, and if not installed in accordance with the manufacturer's instructions, may cause radio frequency interference.

This equipment complies with Part 15, Subpart J of the FCC rules for a Class A computing device. This equipment also complies with the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of the Canadian Department of Communications. These above rules are designed to provide reasonable protection against such interference when operating the equipment in a commercial environment. If operation of this equipment in a residential area causes radio frequency interference, the user, and not Minicom Advanced Systems Limited, will be responsible.

Changes or modifications made to this equipment not expressly approved by Minicom Advanced Systems Limited could void the user's authority to operate the equipment.

1.6 Safety

The device must only be opened by an authorized Minicom technician. Disconnect the device from the power source and all cables from the device before service operation!

1.7 User Guide Feedback

Your feedback is very important to help us improve our documentation. Please email any comments to: ug.comments@minicom.com.

Please include the following information:

- Guide name
- Part number
- Version number (on the front cover)

1.8 Trademarks

All trademarks and registered trademarks are the property of their respective owners.

1.9 WEEE Compliance

This section provides WEEE Information for Minicom Customers and Recyclers.

Under the Waste Electrical and Electronic Equipment (WEEE) Directive and implementing regulations, when customers buy new electrical and electronic equipment from Minicom, they are entitled to:

- Send old equipment for recycling on a one-for-one, like-for-like basis (this varies depending on the country)
- Send back the new equipment for recycling when it ultimately becomes waste

Instructions for both customers and recyclers / treatment facilities wishing to obtain disassembly information are provided in our website www.minicom.com.

2 Installation

2.1 Overview

Install the Smart 108/116 IP system as follows:

1. Remove the Smart 108/116 IP system from the package, and check that all components are present and in good working condition.
2. Mount the Smart 108/116 IP unit in a rack.
3. Make all hardware connections between the power source, Smart 108/116 IP, services, network, and KVM console.
4. Power on the Smart 108/116 IP unit.

2.2 System Components

Before installing the Smart 108/116 IP system, verify that you have all the components on the following list, as well as any other items required for installation.

The Smart 108/116 IP system consists of:

- One Smart 108 IP (p/n 0SU70032) or one Smart 116 IP (p/n 0SU60005)
- One RS232 Download cable (p/n 5CB40419)
- ROCS - PS/2, USB (ordered separately)
- CAT5 cables (1.5 m provided)
- A rack mounting kit (p/n 5AC20247)

2.2.1 The Smart 108/116 IP Unit

The Smart 108/116 IP Unit front panel is illustrated in Figure 1.

Figure 1 – Smart 108/116 IP Unit Front Panel

The following table describes the functionality of the LEDS and buttons on the front panel of the Smart 108/116 IP.

LED/Button	Functionality
Power LED	Indicates the state of the Smart 108/116 IP unit: Green indicates that the unit is powered on; Red indicates that the unit is powered off.
Remote LED	Illuminates to indicate that a remote session is active.
Link	Illuminates to indicate that the unit is connected to the network.
Local button	When pressed, Smart 108/116 IP disconnects the client remote session, and the local mouse and keyboard become operational. The **Remote** LED turns off.
Reset	Pressing and holding this button for more than seven seconds, resets the Smart 108/116 IP Unit.

The Smart 116 IP Unit rear panel is illustrated in Figure 2; it has sixteen server ports. The Smart 108 IP is the same, with the exception that it has eight server ports.

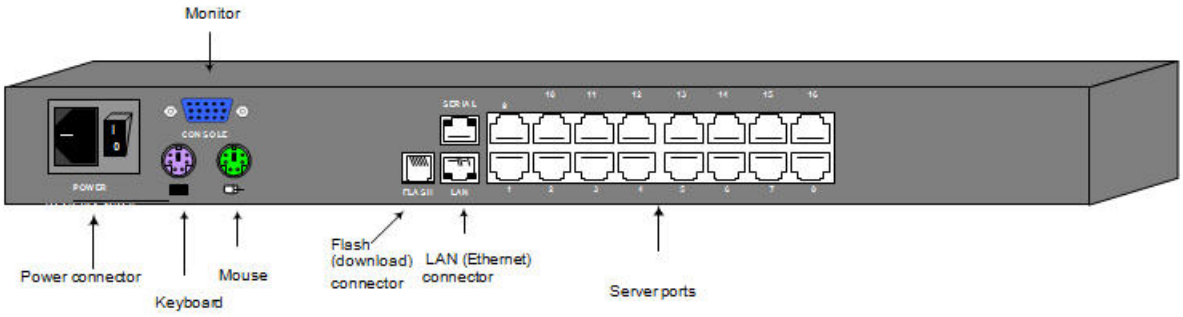


Figure 2 – Smart 116 IP Unit Rear Panel

The following table describes the functionality of the ports on the rear panel of the Smart 108/116.

Port	Functionality
Console KVM	For connecting a keyboard, video, and mouse to operate the Smart 108/116 IP locally; optional.
Serial	Not in use
Flash	For updating firmware of the analogue part of the Smart 108/116 IP system - OSD, Switch, RICCs, and ROCs.
LAN	For connecting to the 10/100 Mbit Ethernet. The LED illuminates green when the unit is connected to a 100 Mbit/sec network; it illuminates yellow when the unit is connected to a 10 Mbit/sec network.
Server ports	For connecting to the servers via the RICC/ROCs.

2.3 Pre-Installation Guidelines

- Place cables away from fluorescent lights, air conditioners, and machines that are likely to generate electrical noise.
- Place the Smart 108/116 IP unit on a flat, clean and dry surface.
- The Smart 108/116 IP unit is not intended for connection to exposed outdoor lines.
- Ensure that the maximum distance between each computer and the Smart 108/116 IP unit, does not exceed 10 m / 33 ft for RICCs, and 30 m/100 ft for ROCs.

2.4 Rack Mounting the Smart 108/116 IP Unit

2.4.1 Rack Mounting Safety Considerations

When mounting Smart 108/116 IP onto a rack, avoid the following conditions:

- **Elevated operating ambient temperature** – The operating ambient temperature of the rack environment may be greater than the room ambient temperature. Therefore, take special care when installing the unit in a closed or multi-unit rack assembly that the environment is compatible with the maximum rated ambient temperature.
- **Reduced airflow** – Install the equipment in a rack in such a way that the amount of airflow required for safe operation is not compromised. Leave a gap of at least 5 cm / 2” on each side of Smart 108/116 IP.
- **Uneven mechanical loading** – Uneven loading can cause damage to the equipment or personal injury. Mount the equipment in the rack in such a way that a hazardous condition does not result due to uneven mechanical loading.
- **Circuit overloading** – When connecting the equipment to the supply circuit, make sure that the total power of all the components does not exceed the circuit capabilities. Overloading of circuits can affect over-current protection and supply wiring, potentially resulting in fire and shock hazards.
- **Unreliable earthing** – Maintain reliable earthing of rack-mounted equipment. Pay attention to supply connections other than direct connections to the branch circuit (for example, use of power strips).

2.4.2 Mounting the Unit

You can connect the Smart 108/116 IP unit to a server rack, using the supplied rack mounting kit. The brackets can be placed in two possible positions, as illustrated in the following figure.

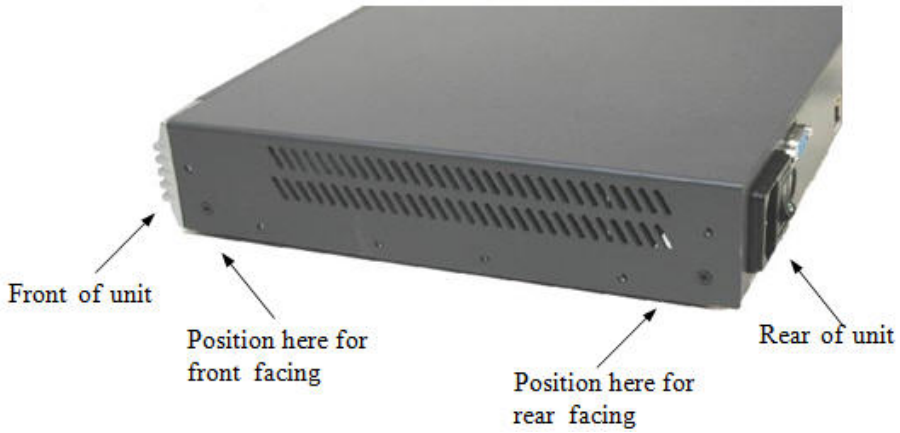


Figure 3 – Bracket Positions

➔ **To rack mount the Smart 108/116 IP unit:**

1. Place the brackets on the unit in either of the following ways:
   - Towards the front of the unit so that the unit can be mounted front facing
   - Towards the rear of the unit so that the unit can be mounted rear facing

   Figure 4 illustrates the bracket connected for rear facing.
2. Screw the bracket to the Smart 108/116 IP unit using the screws provided.

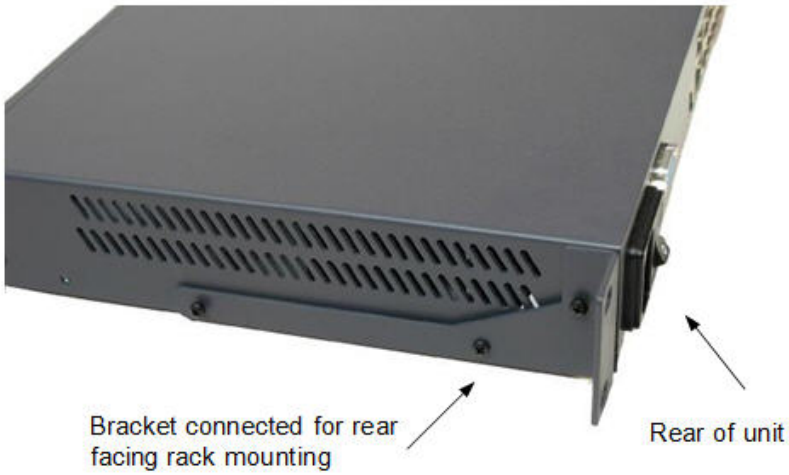


Figure 4 – Bracket Connected for Rear Facing

3. Install the Smart 108/116 IP nit into the server rack by connecting the bracket to the rack with screws, according to the rack manufacturer's instructions.

2.5 Connecting the System

Figure 5 illustrates the Smart 108/116 IP system overview.

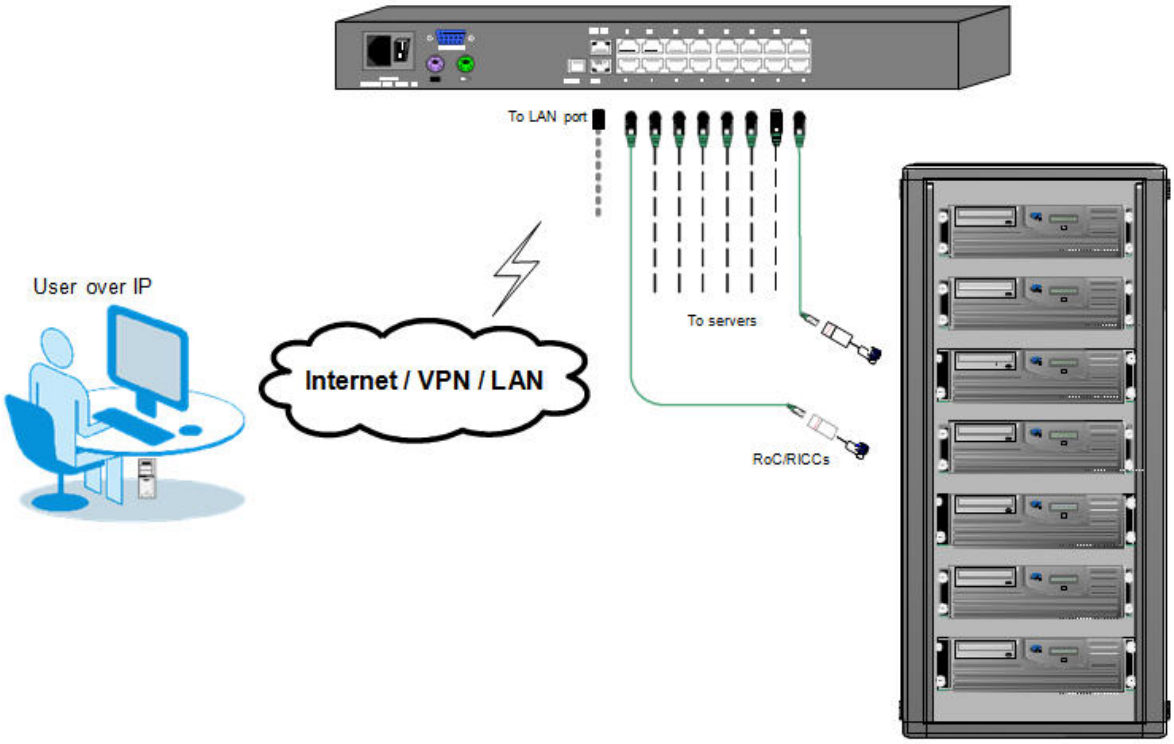


Figure 5 – Smart 108/116 IP System Overview

2.6 Connecting to the Servers

Each computer/server is directly connected to the Smart 108/116 IP via an appropriate ROC or RICC using a CAT5 cable in star configuration. No external power is needed at the remote RICC/ROCs. The RICC/ROCs draw their power from the computer's keyboard port (RICC/ROC PS/2, SUN) or from the USB port (RICC/ROC USB). Figure 6 and Figure 7 illustrate the ROC PS/2 and ROC USB.

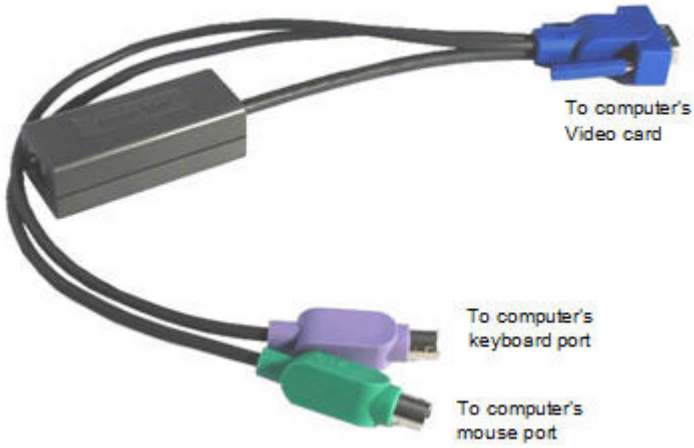


Figure 6 – ROC PS/2

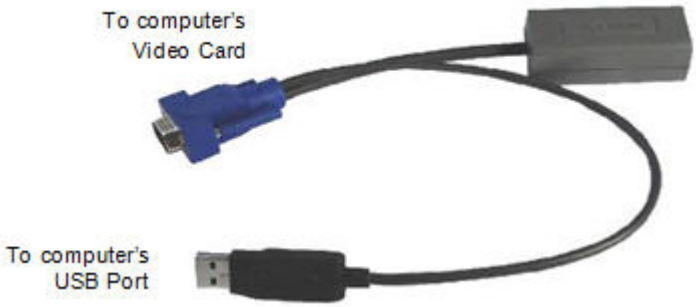


Figure 7 – ROC USB

2.6.1 Connecting a RICC/ROC PS/2

The connections for the RICC PS/2 and ROC PS/2 are exactly the same.

The following figure illustrates the RICC PS/2.

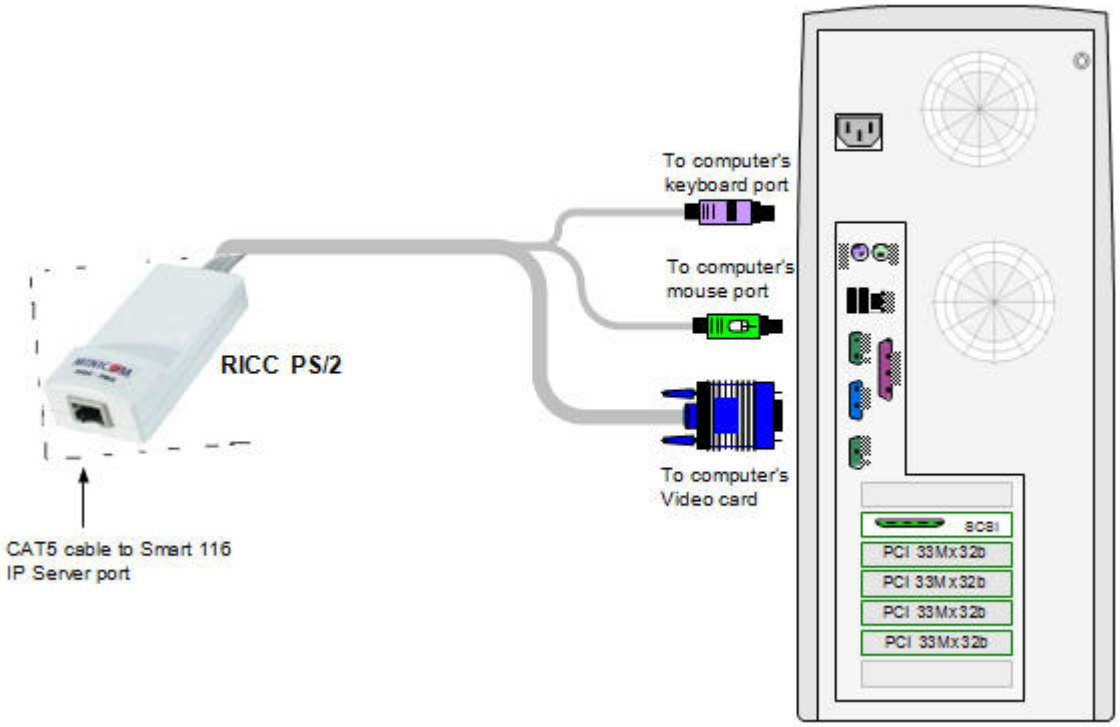


Figure 8 – RICC PS/2 Connections

You can connect the RICC/ROC PS/2 to a powered on computer, by performing the steps of the following procedure in order.

➔ **To connect the RICC/ROC PS/2 to a powered on computer:**

1. Connect the Mouse connector to the computer's Mouse port.
2. Connect the Keyboard connector to the computer's Keyboard port.
3. Connect the Screen connector to the computer's Video card.

Failure to connect in the above order while the server is running may lead to the mouse malfunctioning until the server is rebooted.

2.6.2 Connecting a RICC/ROC USB

The RICC/ROC USB supports Windows 98 SE and later, MAC, SUN, and SGI, and all modern Linux distributions. The connections for the RICC USB are exactly the same as for the ROC USB.

The following figure illustrates the RICC USB and its connections.

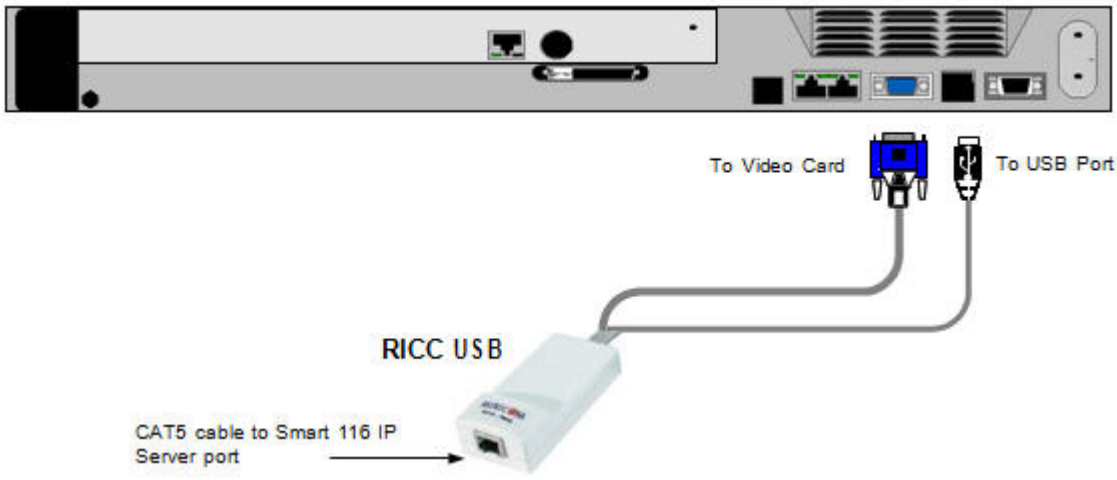


Figure 9 – RICC USB

➔ **To connect the RICC/ROC USB:**

1. Connect the Screen connector to the computer's video card.
2. Connect the USB connector to the computer's USB port.

2.6.3 Connecting a RICC SUN

The following figure illustrates the RICC SUN and its connections.

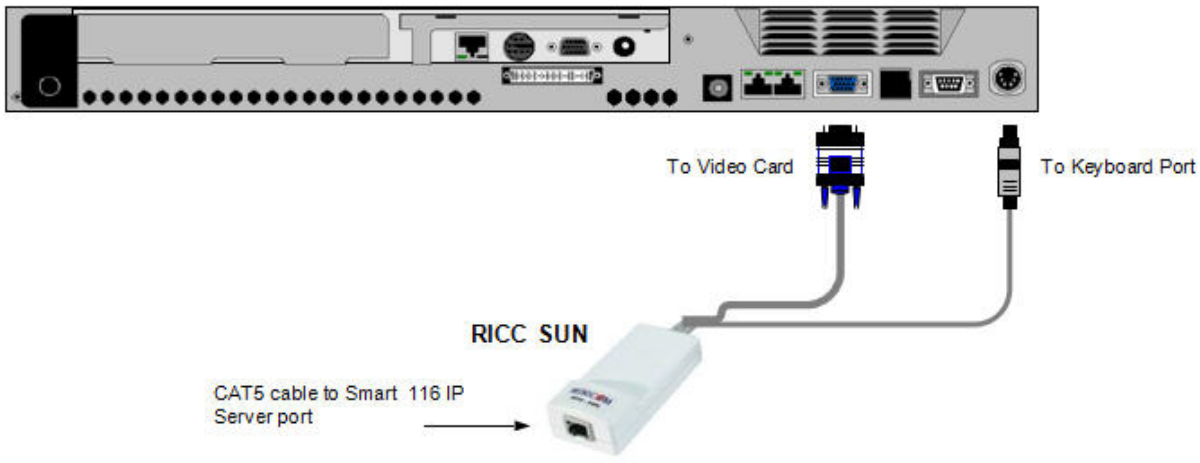


Figure 10 – RICC SUN

➔ **To connect the RICC SUN:**

1. Connect the Screen connector to the computer's video card.
2. Connect the Keyboard connector to the computer's Keyboard port.

2.7 Connecting to the Network

Before powering on Smart 108/116 IP, you can connect the Smart 108/116 IP to the network.

➔ **To connect the Smart 108/116 IP to the network:**

1. Connect the network cable to the LAN port of the Smart 108/116 IP.

2.8 Connecting the CAT5 Cables

Perform the following procedure for each computer to which you want to connect CAT5 cables.

➔ **To connect the CAT5 cables:**

1. Connect one connector to the RICC/ROC RJ45 port.
2. Connect the other connector to one of the Smart 108/116 IP computer ports.

2.9 Connecting the KVM Console

You can connect a KVM console to Smart 108/116 IP, in order to operate the system locally.

➔ **To connect a KVM console to Smart 108/116 IP:**

1. Connect the monitor's connector to the Smart 108/116 IP's Monitor port.
2. Connect the keyboard's connector to the Smart 108/116 IP's Keyboard port.
3. Connect the mouse's connector to the Smart 108/116 IP's Mouse port.

2.10 Connecting the Power Supply

➔ **To connect the power supply to Smart 108/116 IP:**

1. Using the power cord provided, connect Smart 108/116 IP to a socket outlet with a grounding connection.

Only use the power cord supplied with the unit.

2. Switch on Smart 108/116 IP.

3 Configuring the Network

After the system has been installed and all connections have been made, you must configure the Smart 108/116 IP system as follows:

1. Configure Smart 108/116 IP's network settings, which includes configuring:
   - Device ID settings
   - Smart 108/116 IP's IP address
   - Centralized Management
2. Configure the SNMP settings.
3. Add, edit, remove, and block system Users.
4. Configure the KVM switch settings.
5. Configure the security settings.

You can also perform the following additional operations, as required:

1. Install an SSL certificate.
2. Upgrade firmware.
3. Restore factory settings.

3.1 Boot-Up Process

By default, Smart 108/116 IP boots with an automatically assigned IP address from a DHCP (Dynamic Host Configuration Protocol) server on the network (see Figure 11 for an overview of the boot-up process). The DHCP server assigns the Smart 108/116 IP a valid IP address, gateway address, and subnet mask.

This automatically assigned IP address can be identified according to the Smart 108/116 IP MAC address that appears on the underside of the Smart 108/116 IP box, next to the device number (D.N.).

If no DHCP server is found on the network, Smart 108/116 IP boots with the static IP address: 192.168.0.155.

If a DHCP server later becomes available, the unit picks up the IP settings from the DHCP server. To keep the static IP address, you can disable DHCP, as explained in Section 3.3.2 on page 30.

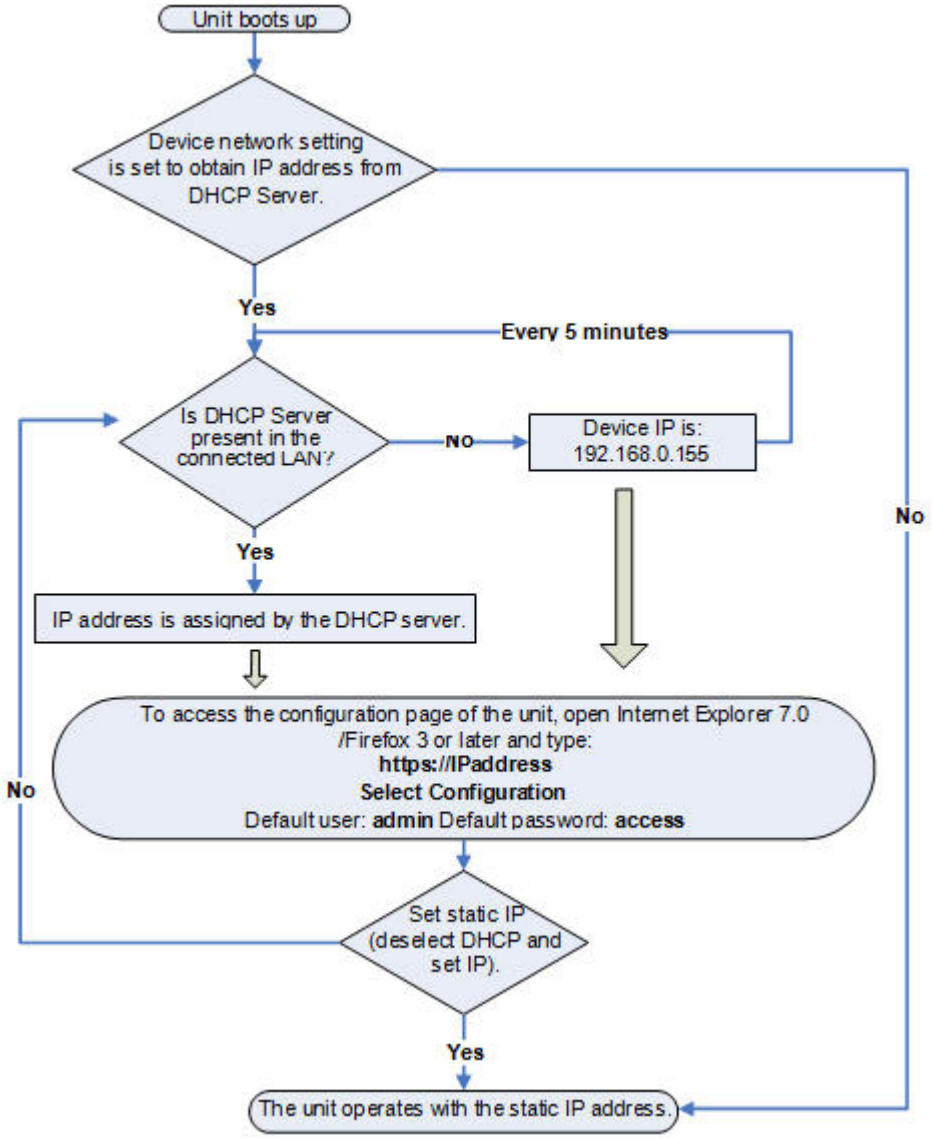


Figure 11 – Boot-Up Process

Assigning Static IP Addresses for a Number of Units

You can connect more than one Smart 108/116 IP to the same network. If there is no DHCP server, or you want to use static IP addresses, connect the Smart 108/116 IP units one at a time and change the static IP address of each unit before connecting the next unit.

3.2 Logging Onto the Web Configuration Interface

You can complete the initial setup of the Smart 108/116 IP system via the Web configuration interface.

Only one Administrator at a time can log onto the Web configuration interface. An idle timeout of 30 minutes terminates the session.

Before logging on the first time, verify that you have the latest Java installed on your computer. If not, you can download and install Java from: http://www.java.com/en/download/index.jsp

➔ **To log into the Web interface:**

1. Open your Web browser (Internet Explorer 7.0 / Firefox 3 or later).
2. Type the Smart 108/116 IP system IP address https://IP address/, and press **Enter**.

   The Web page appears.

Figure 12 – Web Page

3. Click **Log On**.

   Java installs. After installation has completed, the logon page appears.

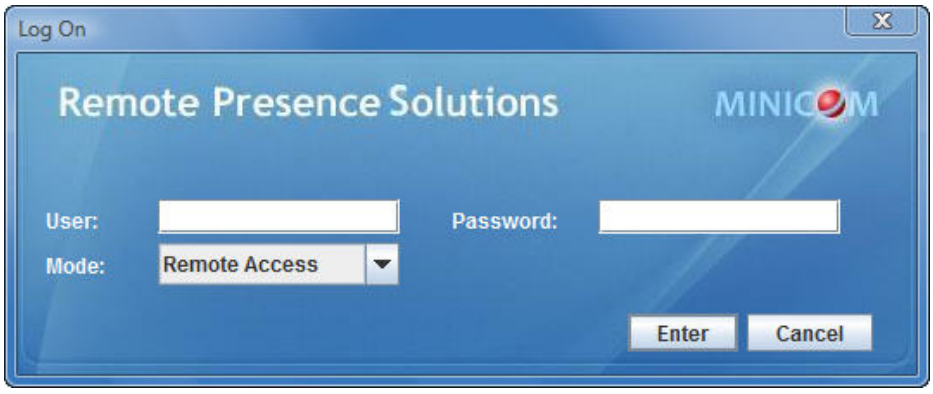


Figure 13 – Logon Page

4. In **User**, type the default Administrator name **admin** and in **Password**, type **access** (both lower case).
5. In **Mode**, select **Configuration**.
6. Click **Enter**.

   The Network configuration page appears with the Device tab open.

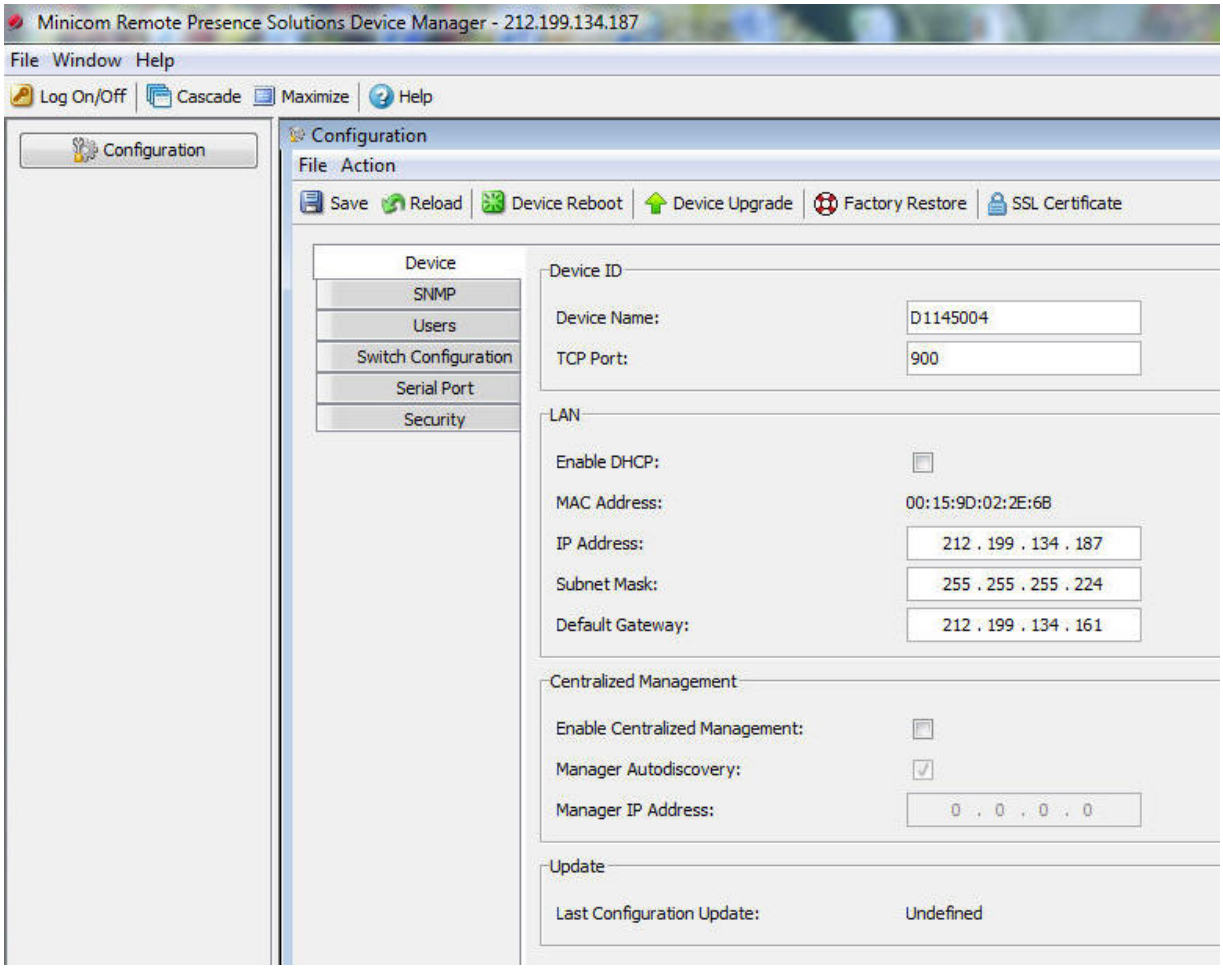


Figure 14 – Network Configuration – Device Tab

From the Configuration menu, you can configure the network, SNMP, Users, Switch Configuration, and Security settings. **After making all configuration changes, you must click the** 

button in the toolbar for the changes to go into effect.

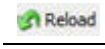
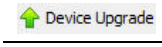
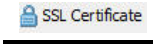
3.2.1 Web Configuration Interface Tabs

The following table summarizes the Web configuration interface tabs.

Tab	Description
Device	For configuration of the device settings, IP address, and centralized management
SMNP	For configuration of network SNMP settings
Users	For adding, editing, deleting, and blocking system Users
Switch Configuration	For configuration of the KVM switch settings
Serial Port	Not in use
Security	For configuration of the security settings

3.2.2 Web Configuration Toolbar Buttons

The following table describes the functionality of the Web configuration toolbar buttons.

Button	Functionality
	Saves the configuration changes
	Reloads the device settings into the configuration page parameter settings
	Reboots the device
	Upgrades the device firmware
	Restores the device with factory settings
	Installs the SSL certificate onto the device

3.3 Configuring the Network Settings

On the network configuration page (see Figure 14), you can configure the following:

- Device ID
- Device IP address
- Centralized Management

Consult your Network Administrator for the network settings.

3.3.1 Configuring Device ID Settings

You can assign a name to the Smart 108/116 IP device, and select a TCP port.

The default device name consists of the letter 'D' followed by the 6-digit device number (D.N.), which is printed on the silver label on the underside of the Smart 108/116 IP box.

If the DHCP server is published in the DNS server, you can connect to the Smart 108/116 IP system using the device name, as follows: https://DeviceName.

You can select any TCP port from port # 800 to 65535. When managed by Centralized Management, the port number can be changed from the management interface, if needed.

Firewall or router security access list must enable inbound communication through the selected TCP port for the Smart 108/116 IP's IP address. (Default TCP port is 900; default Web interface TCP port is 443.)

For client computer access from a secured LAN, the selected ports should be open for outbound communication.

➔ **To configure Device ID settings:**

1. In **Device Name**, type a name for Smart 108/116 IP.
2. In **TCP Port**, type the number of the port (from 800 to 65535).

3.3.2 Configuring the Device IP Address

When a DHCP server is active on the same network to which Smart 108/116 IP is connected, the DHCP can provide automatic IP assignment. However, best practices recommend using MAC address reservations in the DHCP server to ensure that the IP address of the Smart 108/116 IP will not be changed.

Consult your Network Administrator regarding the use of the DHCP.

If you have access to the server, your configured (or default) Smart 108/116 IP device name will appear on the DHCP server's interface, making it easy to locate.

➔ **To configure the device IP address, do one of the following:**

- **Select automatic IP address assignment** – Select the **Enable DHCP** checkbox to enable a DHCP server that is active on the same network to which Smart 108/116 IP is connected, to provide automatic IP assignment.
- **Select manual IP address assignment** – Clear the **Enable DHCP** checkbox to disable the DHCP, and then type the **IP Address**, **Subnet Mask**, and **Default Gateway** for **LAN 1**, provided by your Network Administrator.

3.3.3 Configuring Centralized Management Settings

Minicom's Centralized Management IP-based systems ensure secure control of servers and network devices, and power and user administration in the data center

environment. The Centralized Management systems combine out-of-band KVM via IP access with modern IT standards and requirements. They are the most comprehensive remote server maintenance solutions available in the market today.

➔ **To configure Centralized Management settings:**

1. Select the **Enable Centralized Management** checkbox to enable Smart 108/116 IP to be remotely managed by a Centralized Management system.

   When managed by Centralized Management, only Network Configuration is available from the Smart 108/116 IP configuration page. All other settings, such as Device Upgrade, Factory Restore, and SSL Certificate are disabled and are managed from Centralized Management.

2. Select the **Manager Auto Discovery** checkbox to cause the Centralized Management system to automatically detect Smart 108/116 IP, if they both reside on the same network segment.

   OR

   In **Manager IP Address**, type the static IP address of the Centralized Management Manager.

Although not required, it is recommended to type the **Manager IP Address** even if the Smart 108/116 IP resides on the same network segment as the Centralized Management Manager.

3.4 Configuring Network SNMP Settings

You can activate SNMP logging to provide support network monitoring. This will cause the Smart 108/116 IP to send monitoring events (such as log entries) to the SNMP server. See Chapter 9 for a list of all recorded SNMP events.

➔ **To enable and configure SNMP logging:**

1. From the configuration menu, select **SNMP**.

   The SNMP page opens.

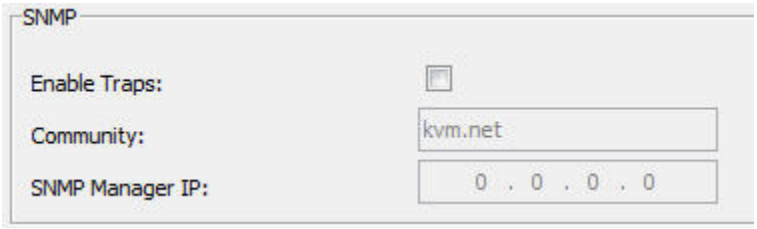


Figure 15 – SNMP Settings

2. Select the **Enable Traps** checkbox to enable SNMP traps of Smart 108/116 IP events and operation.
3. In **Community,** type the name of the SNMP community.
4. In **SNMP Manager IP**, type the SNMP Server IP address.

3.5 Configuring User Settings

An Administrator can add, edit, remove, and block Users.

There are two levels of user access:

- **Administrator** – has unrestricted access to all windows and settings, and can change the name and password of all users
- **User** – can access and control target servers, but cannot use advanced mouse settings and power cycle; cannot access the Web configuration interface

3.5.1 Adding a User

➔ **To add a User:**

1. From the configuration menu, select **Users**.

   The Users page opens and displays the existing Users.

Figure 16 – Users Page

2. Click the **Add** button.

   The Add User page appears.

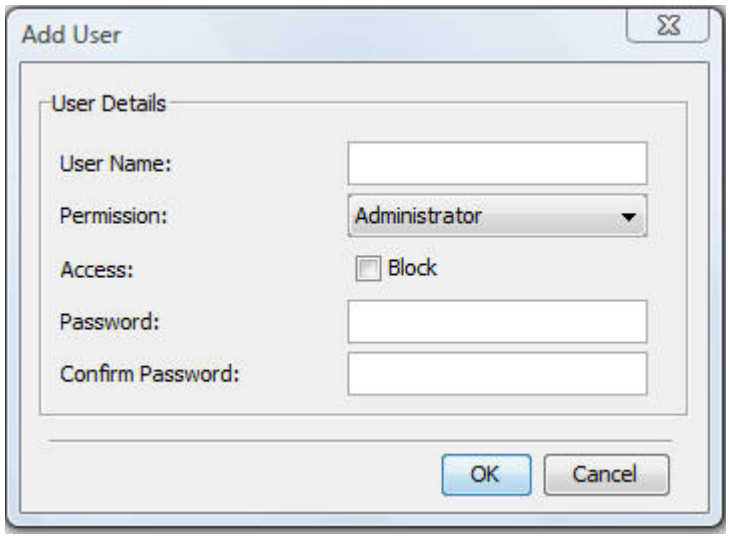


Figure 17 – Add User Page

3. Type a **User Name** and **Password**. The password must be at least six alphanumeric characters long and cannot include the user name, even if other characters are added.

> The "special" characters **&**, **<**, **>**, and " cannot be used for either the user name or password.
>
> The **User Name** and **Password** parameters depend on the security level chosen (see Section 3.7 on page 36).

4. In **Confirm Password**, retype the password.
5. In the **Permission** dropdown menu, select the permission type: **Administrator** or **User**.
6. Click **OK**.

   The User is added to the list of Users.

3.5.2 Deleting User(s)

You can delete one or multiple Users at a time from the system.

> You cannot delete an Administrator who is logged onto the system.

➔ **To delete a User:**

1. In the **Users** page (see Figure 16), select User(s) to delete. Select a group of Users by selecting the first User in the group, pressing the **Shift** button, and then selecting the last User.
2. Click the **Delete** button.

   The Delete confirmation page appears.

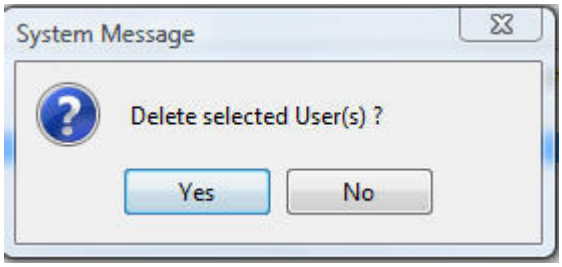


Figure 18 – Delete User Confirmation

3. Click **Yes**.

   The User(s) are deleted from the system.

3.5.3 Blocking a User

An alternative to deleting a User is blocking a User. This means that the User's name and password is stored, but the User is unable to access the system.

➔ **To block a User:**

1. In the **Add User** page (see Figure 17), in the **Access** parameter, select the **Block** checkbox.

3.5.4 Editing User Information

You can change any of the following User parameters: **Permission**, **Access**, and **Password**.

➔ **To edit User information:**

1. In the **Users** page (see Figure 16), select a User and click the **Edit** button.

   The Edit User page appears, with the User's information in the parameters.

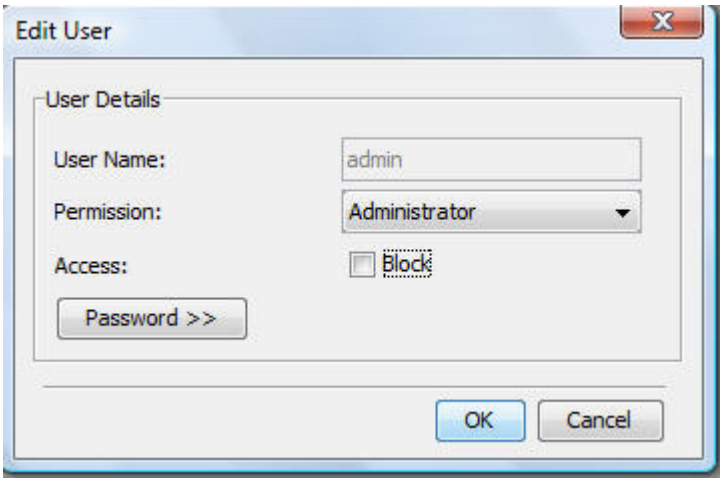
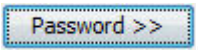


Figure 19 – Edit User Page

2. Change the **Permission** and/or **Access** as required.
3. To change the password, click  .

   The **Password** parameter opens. In the upper textbox, type the new password; in the lower textbox, confirm the new password.

You cannot change the password of an Administrator who is currently logged on to the system.

4. Click **OK**.

   The User page opens with the user information changed accordingly.

3.6 Configuring the KVM Switch

When a KVM switch is connected to the Smart 108/116 IP system, configure the following switch parameters:

- The names of the servers connected to the KVM switch – It is recommended to give the servers connected to Smart 108/116 IP unique names, so that users accessing the system can easily identify the servers.

➔ **To configure a KVM switch:**

1. From the configuration menu, select **Switch Configuration**.

   The KVM Switch Configuration page appears.

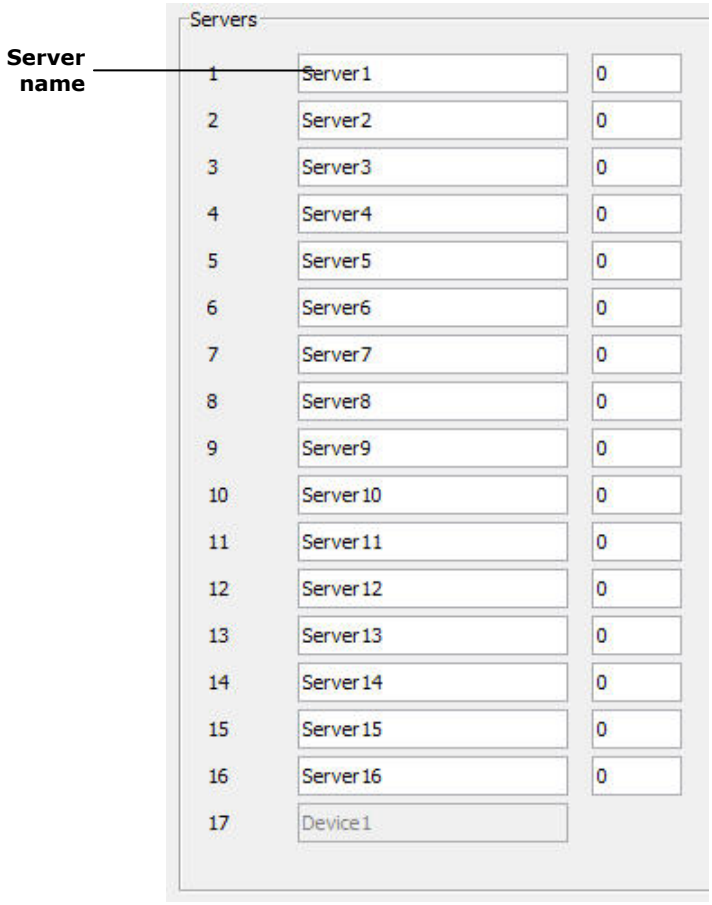


Figure 20 – KVM Switch Configuration Page for Smart 116 IP

The servers that are connected to the selected KVM switch, appear in the **Servers** section. The number of servers that appear corresponds to the number of ports in the KVM switch – 16 for Smart 116 IP; 8 for Smart 108 IP.

The following information is displayed for each potential server:

- The server number
- The server name

2. To change the name of a connected server, highlight the current server name, and type a new name.

3.7 Configuring the Security Settings

This section describes how to configure the security features, such as Account Blocking, Password Policy, and Idle Timeout.

You can choose a standard or high security level of password. The following table describes both these options.

Standard Security Policy	High Security Policy
At least six characters	At least eight characters; must include at least one digit, one uppercase letter, and one of the following "special" characters: **!**, **@**, **#**, **$**, **%**, **^**, *, **()**, **_**, **-**, **+**, **=**, **[]**, ', **:**, **;**, **?**, /, or **{}**
Must not include the user name	Must not include the user name

➔ **To configure the security settings:**

1. From the configuration menu, select **Security**.

   The Security page appears.

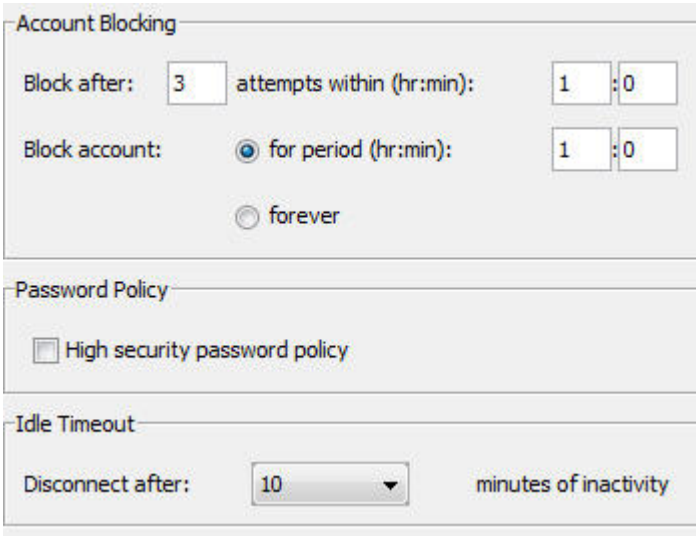


Figure 21 – Security Page

2. In the **Account Blocking** section:

   - In **Block after**, type the number of allowable attempts to log in with a wrong username or password in a time period specified in **attempts within**, prior to a forced time lock.

   - In **Block account**, select **for period** to block the account for a specified period of time, or **forever** for a total block.

3. Select the **High security password policy** checkbox to enable the high security password policy; clear the checkbox for the standard security policy to apply.
4. In **Disconnect after**, select the timeout inactivity period after which the user is disconnected from the system. Select **No Timeout** to disable timeout.

3.8 Performing Additional Configuration Operations

You can perform the following additional operations on Smart 108/116 IP:

- Install an SSL certificate.
- Upgrade firmware.
- Restore factory settings.

3.8.1 Installing an SSL Certificate

You can install an SSL Certificate, to ensure secure transactions between the Web servers and browsers.

➔ **To install an SSL Certificate:**

1. In the toolbar, select SSL Certificate.

   The SSL Certificate page appears.

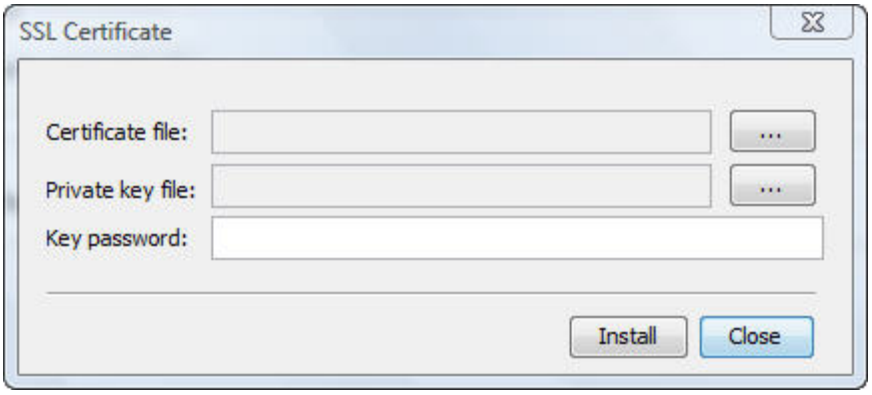


Figure 22 – SSL Certificate Page

2. In **Certificate file**, browse to locate the **Cer** file.
3. In **Private key file**, locate the **private key** file in Microsoft pvk format.
4. In **Key password**, type the password required to upload the Private Key file.

Each Private Key file is generated with a unique password.

5. Click **Install**.

   The SSL Certificate is installed.

6. Save the changes and restart the system, by clicking the Save button, and then the Device Reboot button.

3.8.2 Upgrading Firmware

You can upgrade the Smart 108/116 IP firmware to take advantage of new features.

➔ **To upgrade firmware:**

1. Download the firmware from Minicom's website at: http://www.minicom.com/phandlh.htm.
2. Save the firmware file on the client computer.
3. In the toolbar, select Device Upgrade.

   The Device Version Upgrade page appears, displaying the current firmware version on the device.

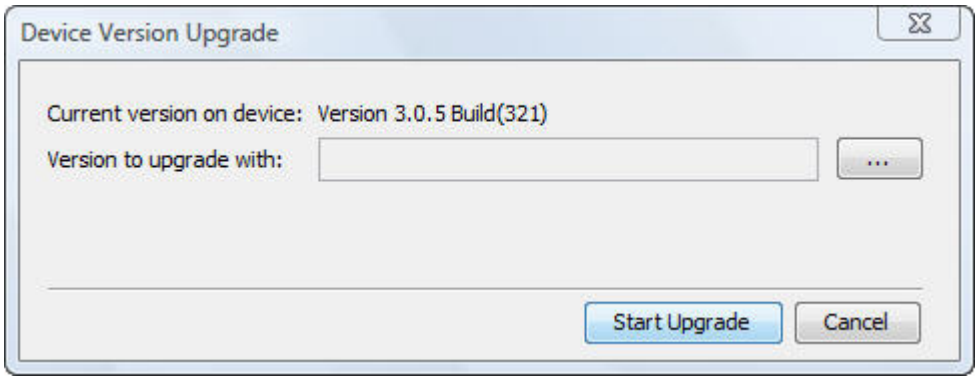


Figure 23 – Device Version Upgrade Page

4. In **Version to upgrade with**, browse to locate and upload the firmware file.
5. Verify the current and uploaded version of the firmware.
6. Click **Start Upgrade**.

   The upgrade starts.

7. On upgrade completion, on the toolbar, click Device Reboot.

   A confirmation box appears.

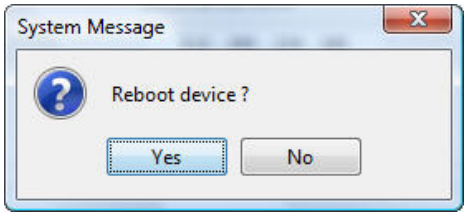


Figure 24 – Reboot Confirmation Page

8. Click **Yes**.

   The unit reboots. After about 30 seconds, the Login page appears.

Depending on the type of firmware upgrade, the following settings may be erased: User settings, KVM switch settings, mouse and video adjustments, and RS232 settings. The network settings remain intact. For more information, refer to the firmware release notes.

3.8.3 Restoring Factory Settings

You can restore the Smart 108/116 IP unit to its factory settings. This restores the original Smart 108/116 IP parameters, resetting all the information added by the administrators, including: Network settings*, Servers, Switches, Users, and Passwords.

- You have the option to preserve Network settings – as explained in the following procedure.

The OSD preserves the server names and other settings. You can restore the OSD settings from the OSD (see Section 0.0.0).

Once reset, the data cannot be retrieved.

➔ **To restore factory settings:**

1. In the toolbar, select Factory Restore.

   The Restore Factory Settings page appears.

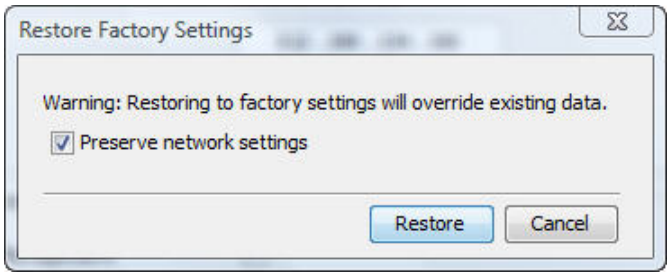


Figure 25 – Restore Factory Settings Page

2. To preserve network settings, select the **Preserve network settings** checkbox.
3. Click **Restore**.

   Factory settings are restored.

3.9 Reloading a Page

You can load the parameters on any configuration page with the settings from the Smart 108/116 IP device. This is convenient if you have already changed settings on the page, and want to restore the device settings.

➔ **To reload a page:**

1. In the Configuration page toolbar, click the Reload button.

   The parameters are populated with the device settings.

3.10 Saving Changes and Logging Out

Once you have completed configuration changes, you must save them.

Changes to the SSL Certificate and Security pages require saving and restarting.

Saving the configuration changes after changing the Device page restarts the unit automatically.

➔ **To save changes:**

1. In the Configuration page toolbar, click the Save button.

   If you made changes to the Device page, the system automatically prompts you to reboot and restart the device, by displaying the following device reboot confirmation box:

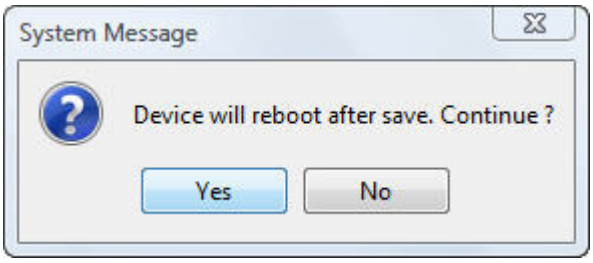


Figure 26 – Device Reboot Confirmation Message

1. Click **Yes**.

   A message box informs that Save has completed.

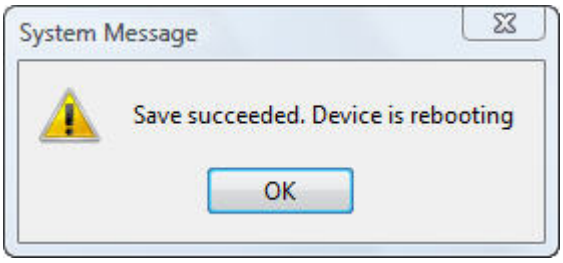


Figure 27 – Save Succeeded Message

2. Click **OK**.

   Device reboots, and when it completes a Logon page appears.

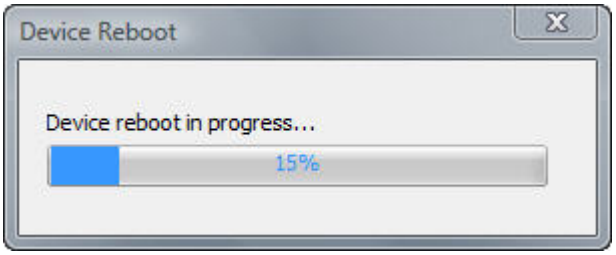


Figure 28 – Device Rebooting Progress Box

Figure 29 – Logon Page after Rebooting

3. Type your **User** name and **Password** and click **Enter**.

   The Configuration page opens.

➔ **To log off:**

1. In the screen toolbar, click the 

button.

   The Configuration screen is closed, and the session closes.

4 Conducting a Remote Session

The remote session enables remotely accessing the server connected to Smart 108/116 IP. Before starting a remote session, Smart 108/116 IP must be fully configured.

You can perform the following from the remote session:

- Display/hide the toolbar.
- Set the session profile.
- Display the session in full screen mode.
- Verify Remote Presence Solutions information.
- Adjust video settings.
- Manage keyboard sequences.
- Synchronize mouse pointers.
- Switch to a different server or device.

4.1 Starting a Remote Session

On first connection, install the Minicom certificate and verify that you have the latest Java installed on your computer. If not, you can download and install Java from: http://www.java.com/en/download/index.jsp

When using the Firefox browser, install the Minicom Firefox add-on.

The following procedure describes how to log into a remote session from a client computer.

➔ **To log onto a remote session:**

1. Open your Web browser (Internet Explorer 7.0 / Firefox 3 or later).
2. Type the Smart 108/116 IP system IP address - https://IP address/ and press **Enter**.

   The Web page appears (see Figure 12).
3. In the Web page, click **Log On**.

   Java installs. After installation has completed, the logon page appears.

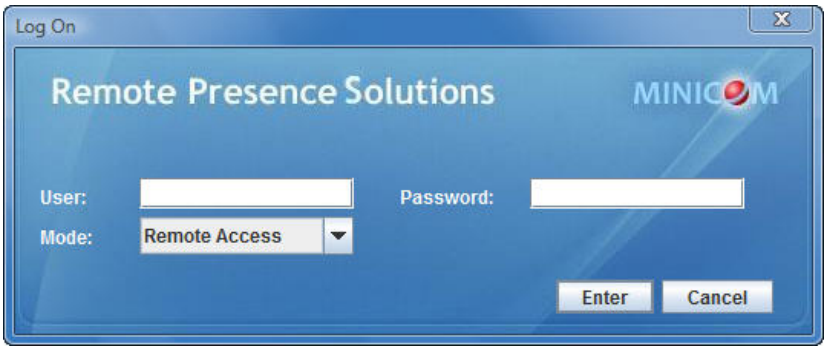


Figure 30 – Logon Page

Leave **Mode** as **Remote Access**.

4. In **User** and **Password**, type the default Administrator name and password, **admin** and **access** respectively (both lower case).
5. Click **Enter**.

   The screen of the target server or the currently selected server on the KVM switch that is connected directly to Smart 108/116 IP, appears with the Smart 108/116 IP toolbar.

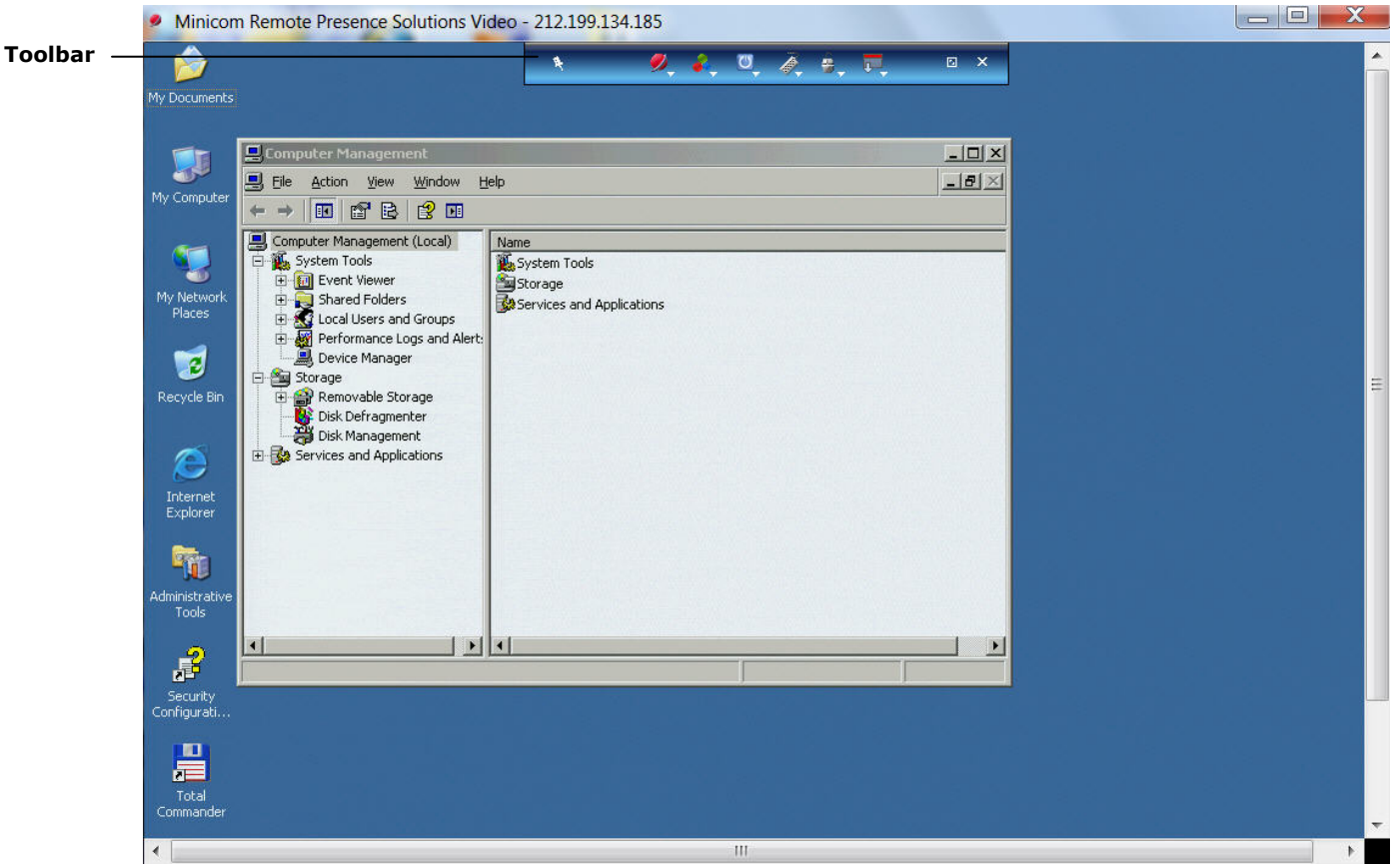


Figure 31 – Remote Session Page

The Remote Session page displays:

- **Server Confirmation label** – This confirms the identity of the current server accessed, and disappears by default after 30 seconds (this period can be adjusted in the OSD, as explained in Section 6.2.6). It appears again when switching to a different server. The currently accessed server identity can be checked any time by looking at the Server name on the remote client menu.

4.1.1 Remote Session Toolbar Buttons

The following table describes the functionality of the Remote Session toolbar buttons.

Button	Description
	Toggle button for displaying/hiding toolbar.
	Session button. Pressing this button opens up a dropdown menu for selecting: **Session Profile** – enables configuring remote session profile session **About** – displays client, firmware, Switch File, and KME version information
	Video button. Pressing this button opens up a dropdown menu for performing: **Refresh** – for refreshing the video image **Video Adjust** – for automatically adjusting the video image **Advanced** – for manually setting video settings **Performance** – changing video performance by changing mode and/or bandwidth
	Keys button. Pressing this button opens up a dropdown menu with predefined key sequence names and **Special Keys** item which enables you to: add a keyboard sequence, record a new custom key, edit an existing key sequence, and delete a key sequence
	Mouse button. Pressing this button opens up a dropdown menu for performing: **Calibrate** – calibrates the speeds of the mouse pointers of the target server and client computer in Win98, NT or 2000 **Align** – for aligning the local mouse pointer with the remote target server mouse pointer **Mouse Settings** – for manually synchronizing the mouse pointers
	Server button. Pressing this button displays the connected servers. You can switch to a different server.
	Restore button. To toggle Full screen mode on and off.
	Logoff button. Closes the current remote session and displays the logon Web page.

4.2 Sharing a Remote Session

Users who want to remotely work on a server at the same time and collaborate their work, can share a remote session. All users in the remote session can connect to see the video at the same time and share the Keyboard/Mouse control. Up to five users can share the same remote session.

When connecting to a target server that other users are already connected to, the following message appears:

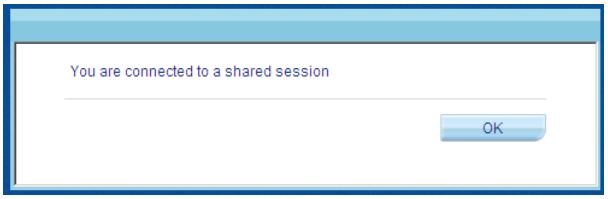


Figure 32 – Shared Remote Session

4.2.1 Exclusive Session

When starting a remote session and there are no other logged in users, a user can prevent other users from connecting to the session (see Section 4.4, step 4). This means that the user is the only one who can see the video and control the Keyboard/Mouse, enabling the user to work on the server without anyone seeing or interfering in the user's work.

4.3 Displaying the Toolbar

The toolbar appears briefly at the top of the screen (see Figure 31). It disappears when the mouse is not over it. To make it reappear, glide the mouse over the top of the screen. To display the toolbar permanently, click the tack icon  on the toolbar.

4.4 Setting the Session Profile

You can set the remote session display features, as follows:

- Select the format of the mouse pointer, or hide it.
- Hide the toolbar.
- Display the session in full screen mode – You can work on the target server as if you are working on a local computer, using full screen mode. In Full Screen mode, the desktop window disappears, and is replaced by the accessed target server desktop.
- Prevent other users from logging into the same session.

➔ **To set the session profile:**

1. On the toolbar, select  **> Session Profile.**

   The Session Profile window appears.

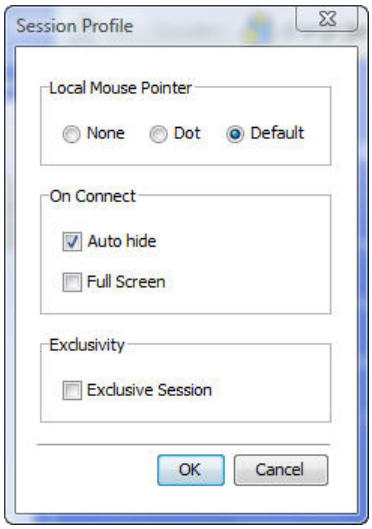


Figure 33 – Session Profile Dialog Box

2. In **Local Mouse Pointer**, select one of the following options to set the appearance of the client computer mouse pointer:
   - **None** – to hide the mouse pointer
   - **Dot** – for the mouse pointer to appear as a dot
   - **Default** – for the mouse pointer to appear as a regular-shaped mouse cursor
3. In **Auto Connect**, select:
   - **Auto hide** – to hide the toolbar from the next connection onwards
   - **Full Screen** – to display the remote session screen in full screen mode from the next connection onwards. To toggle full screen mode on and off, you can click the Restore button  (see Section 4.4.1).
4. In **Exclusivity**, select the **Exclusive Session** checkbox when starting a remote session and there are no other logged in users; this prevents other users from logging into the session.

4.4.1 Full Screen Mode

You can work on the target server as if you are working on a local computer, using full screen mode. In Full Screen mode, the desktop window disappears, and is replaced by the accessed target server desktop.

➔ **To work in full screen mode:**

1. Ensure that the client computer has the same screen resolution as the target server.
2. On the toolbar, click the Restore button  .

   The desktop window disappears.

➔ **To exit full screen mode:**

1. On the toolbar, click the Restore button  .

   The desktop window appears.

Full screen mode can also be activated from the Session Profile box, see Section 4.4, step 3.

4.5 Verifying Remote Presence Solutions Information

You can verify the client, firmware, KME (Keyboard/Mouse Emulation firmware), and Switch file versions installed on your Smart 108/116 IP. This information can assist system administrators in troubleshooting and support.

➔ **To verify Remote Presence Solutions information:**

1. On the toolbar, select  **> About**.

   The information screen appears.

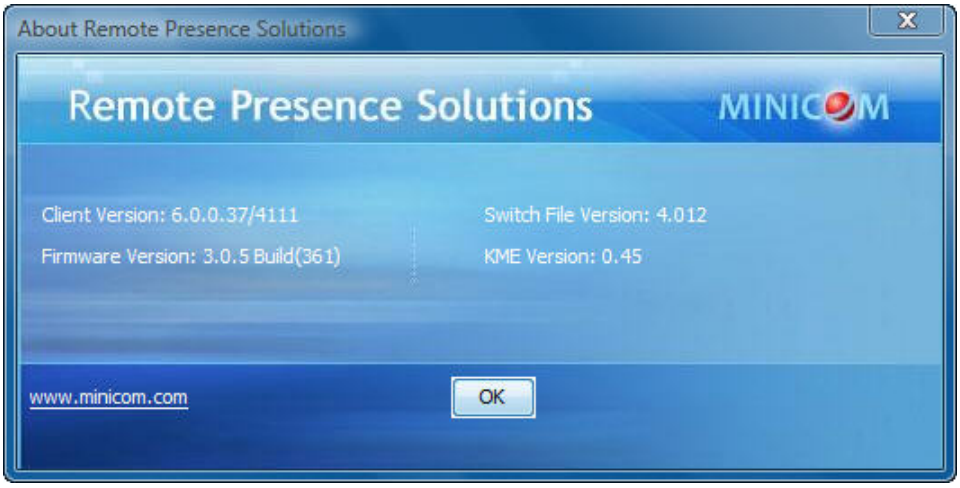


Figure 34 – Remote Presence Solutions Information

4.6 Changing the Video Performance Settings

From the toolbar, you can alter the video performance settings, by selecting a different mode or bandwidth.

The mode can be set to:

- **Fixed** – Enables you to select any bandwidth option. For example, in a LAN environment, it is best to set the bandwidth setting to **High**. For VPN and Internet environments, you may want to alter the settings to increase responsiveness.
- **Adaptive** – Automatically adapts to the best compression and colors according to the network conditions.

You can choose to display more colors for more fidelity, or less colors to reduce the volume of data transferred through the network. Choosing more colors requires more bandwidth.

The bandwidth can be set to:

- **Maximum** – For optimal performance when working on a LAN. This gives no compression and high color (16 bit)
- **High** – For low compression and high color (16 bit)
- **Medium** – For medium compression and either high color or 256 colors; Recommended when using a standard Internet connection
- **Low** – For high compression and 16 colors

➔ **To alter the settings:**

1. On the toolbar, select  **> Performance**.

   The Performance dialog box appears.

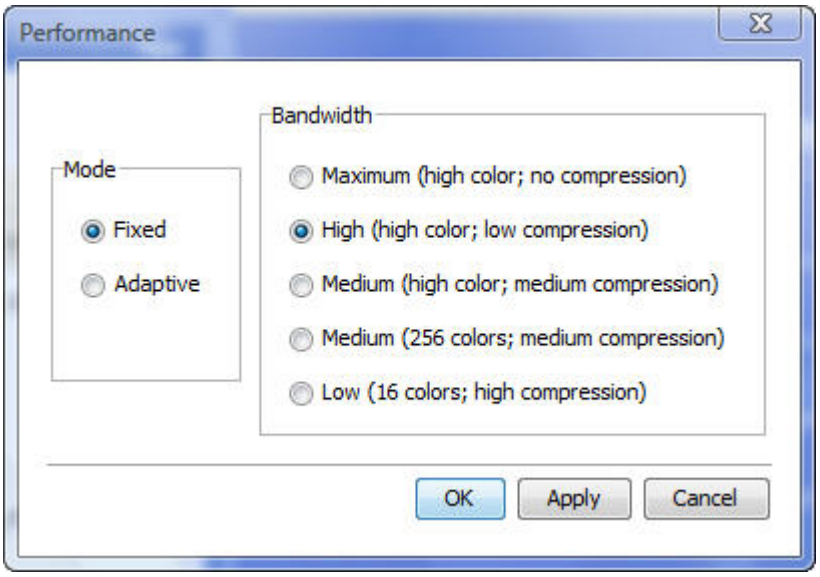


Figure 35 – Performance Settings

2. In **Mode**, select **Fixed** or **Adaptive**.
3. For **Fixed** mode, in **Bandwidth**, select **Maximum**, **High**, **Medium** (high color or 256 colors), or **Low**.
4. Click **OK**.

   The chosen setting takes effect and the screen of the last accessed target server appears.

4.7 Adjusting the Video

There are three ways to adjust the video image:

- Refreshing the video image
- Automatically adjusting the video image
- Manually changing advanced video settings

4.7.1 Refreshing the Video Image

The video image may require refreshing when changing the display attributes of a target server. Refreshing completely regenerates the video image.

➔ **To refresh the video image:**

1. On the toolbar, select  **> Refresh**.

   The image is refreshed.

4.7.2 Automatically Adjusting the Video Image

The video view may need to be adjusted for each target server or new screen resolution. In most cases, adjusting the video view using the default video settings gives the optimal view.

➔ **To automatically adjust the video image:**

1. On the toolbar, select  **> Video Adjust**.

   The progress of video adjustment is displayed.

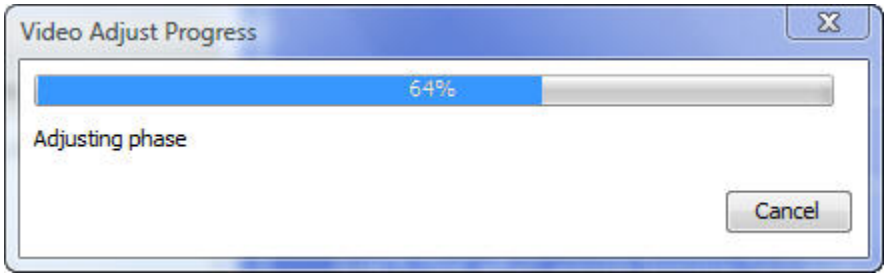


Figure 36 – Video Adjust Progress

   The process takes a few seconds. If the process runs more than a few times, it is an indication that there is an abnormal noise level. Check the video cable and verify that no dynamic video application is running on the target server's desktop.

4.7.3 Manually Adjusting Video Settings

Although automatic adjustment of video generally optimizes the video view, you may want to fine-tune the results.

You can use the advanced video adjustment options:

- To fine-tune the target server video settings after auto adjustment
- To adapt to a noisy environment or a nonstandard VGA signal
- When in full-screen DOS/CLI mode

After adjusting the video settings manually, you can always revert to automatically adjusting the video settings, as explained in Section 4.7.2.

➔ **To manually adjust the video settings:**

1. On the toolbar, select  **> Advanced**.

   The manual controls appear.

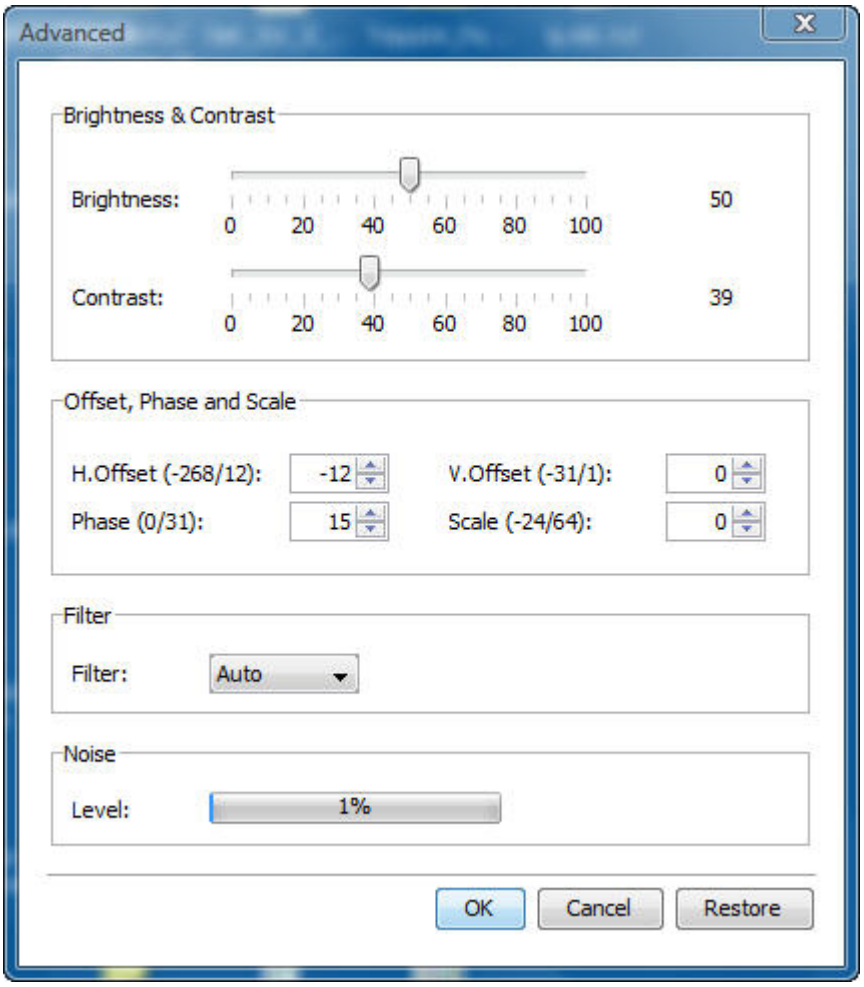


Figure 37 – Manual Video Adjustments Controls

2. In **Brightness** and **Contrast**, use the scales to adjust the brightness and contrast of the displayed image, respectively. Move the sliders to change the displayed image. Click in the area of the sliders for fine-tuning.
3. In the **Offset, Phase and Scale** section:
   - In **H. Offset**, select the starting position of each line on the displayed image.
   - In **V. Offset**, select the vertical starting position of the displayed image.
   - In **Phase**, select the point at which each pixel is sampled.
   - In **Scale**, select the scale resolution of the session image.

   Adjust **Phase** and **Scale** to reduce the noise level to a minimum.
4. In **Filter**, select the filter of the input video from the server. A higher filter reduces the noise level but makes the image heavier. Options are: **Auto**, **No Filter**, **Low**, **Medium**, and **High**.

5. **Level** displays the Video "noise" level when a static screen is displayed.
6. Click **OK**.

4.8 Managing Keyboard Sequences

You can select any keyboard sequence (a combination of keys that performs a specific process) that appears in the dropdown menu of the toolbar button  to send it to the target server to initiate its associated process. For example, selecting **Ctrl-Alt-Del** sends this three-key sequence to the target server to initiate its Shutdown/Login process.

When clicked, these key sequences transmit directly to the target server, and do not affect the client computer.

This section describes how to:

- Add predefined keyboard sequences to the list of keyboard sequences
- Create customized keyboard sequences
- Edit existing keyboard sequences
- Delete existing keyboard sequences

4.8.1 Adding a Keyboard Sequence

You can add predefined keyboard sequences to the list of keyboard sequences that can be accessed directly from the dropdown list of the toolbar item  .

➔ **To add a keyboard sequence:**

1. On the toolbar, click  **> Special Keys.**

   The Special Key Manager box appears.

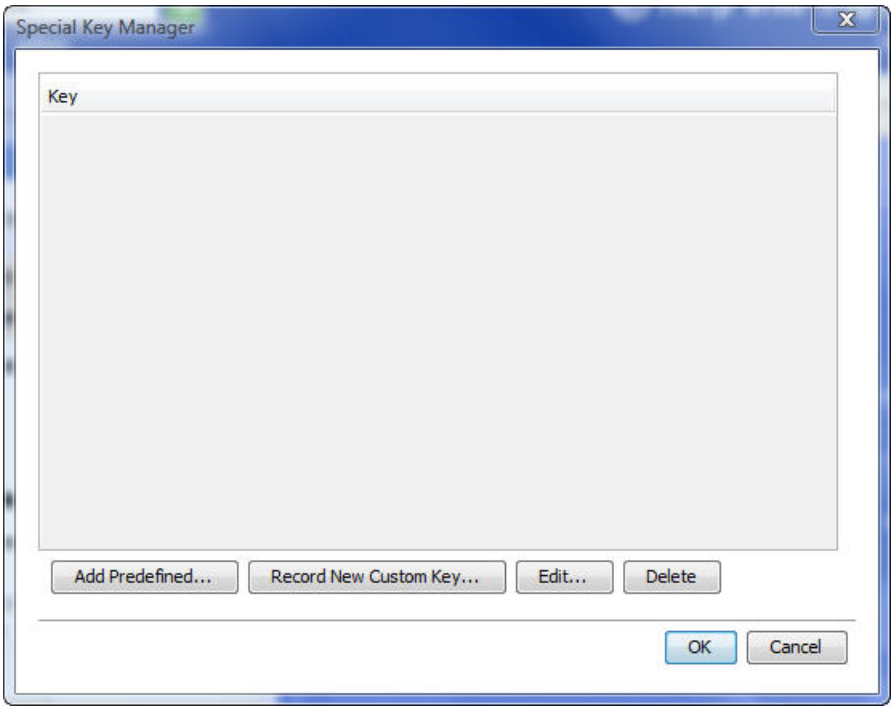


Figure 38 – Special Key Manager

2. Click the **Add Predefined** button.

   A list of existing sequences appears.

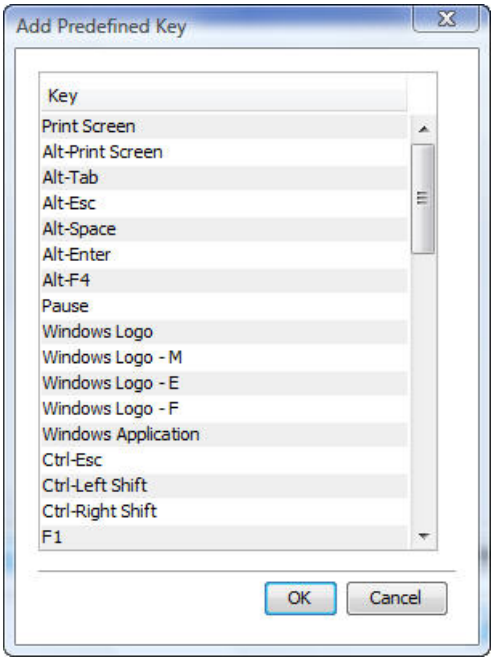


Figure 39 – Add a Predefined Key Dialog Box

3. Select a key sequence and click **OK**.

The sequence appears in the Special Key Manager box.

4. In the Special Key Manager box, click **OK**.

   The sequence appears in the Keyboard Key sequence list.

4.8.2 Recording a New Custom Key

This section describes how to define a new keyboard sequence. After defining the keyboard sequence, you can add it to the list of keyboard sequences that can be accessed directly from the dropdown list of the toolbar item  (see Section 4.8.1).

➔ **To record a keyboard sequence:**

1. In the Special Key Manager box (see Figure 38), click **Record New Custom Key**.

   The Record Macro box appears.

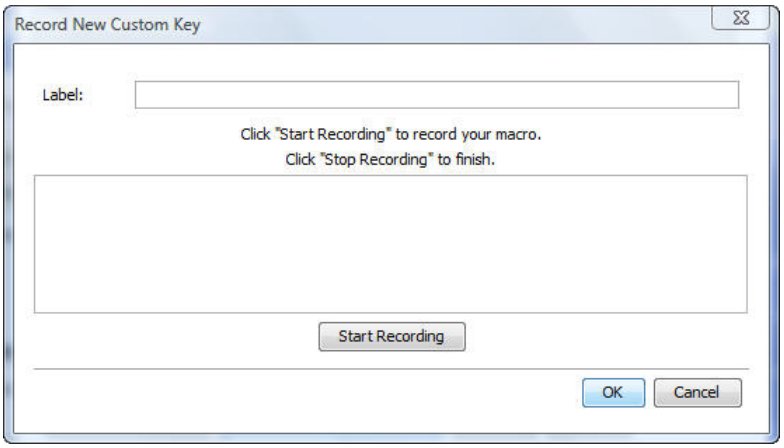


Figure 40 – Record Macro Box

2. In **Label**, type a name for the new key sequence.
3. Click **Start Recording**.
4. On your keyboard, press the keys to include in the key sequence.

   The names of the pressed keys appear in the provided area.

5. Click **Stop Recording**.
6. Click **OK**.

   The new key sequence is now on the list of predefined key sequences.

4.8.3 Editing a Key Sequence

➔ **To edit a predefined keyboard sequence:**

1. In the Special Key Manager box (see Figure 38), select the desired key sequence and click **Edit**.

   The Record Macro box appears (see Figure 40). The name of the key sequence to edit appears in the **Label** field.

2. Click **Start Recording**.
3. On your keyboard, press the keys to include in the key sequence.

   The names of the pressed keys appear in the provided area.

4. Click **Stop Recording**.
5. Click **OK**.

   The key sequence definition is updated in the system.

4.8.4 Deleting Key Sequence(s)

You can delete a single or multiple key sequences from the system.

➔ **To delete a keyboard sequence:**

1. In the Special Key Manager box (see Figure 38), select the desired key sequence(s) to delete. Select a group of keys by selecting the first key in the group, pressing the **Shift** button, and then selecting the last key.
2. Click **Delete**.

   The delete confirmation box appears.

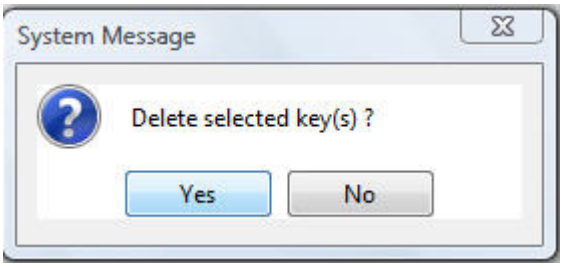


Figure 41 – Delete Key(s) Confirmation Box

4.9 Synchronizing Mouse Pointers

For best mouse performance and superior customer experience, Minicom recommends that you set certain mouse settings in the target operating system. This applies to all targets running Windows, such as XP, Windows 7, Windows Server 2003, and Windows Server 2008.

When working at the client computer, two mouse pointers appear – one of the client computer and one of the target server; the former is on top of the latter. The mouse pointers should be synchronized. The following explains what to do if they are not synchronized.

Before synchronizing mouse pointers, adjust the video of the target server (see Section 4.7); otherwise, mouse synchronization may not work.

4.9.1 Manually Synchronizing the Mouse

If the mouse settings on the target server have been changed, or when the operating system on the target server is Windows XP / 2003 Server / 7 / 2008 Server, Linux, Novell, SCO UNIX, or SUN Solaris, you must synchronize the mouse pointers manually.

➔ **To manually synchronize mouse pointers:**

1. On the toolbar, select  **> Mouse Settings.**

   The Mouse Settings box appears.

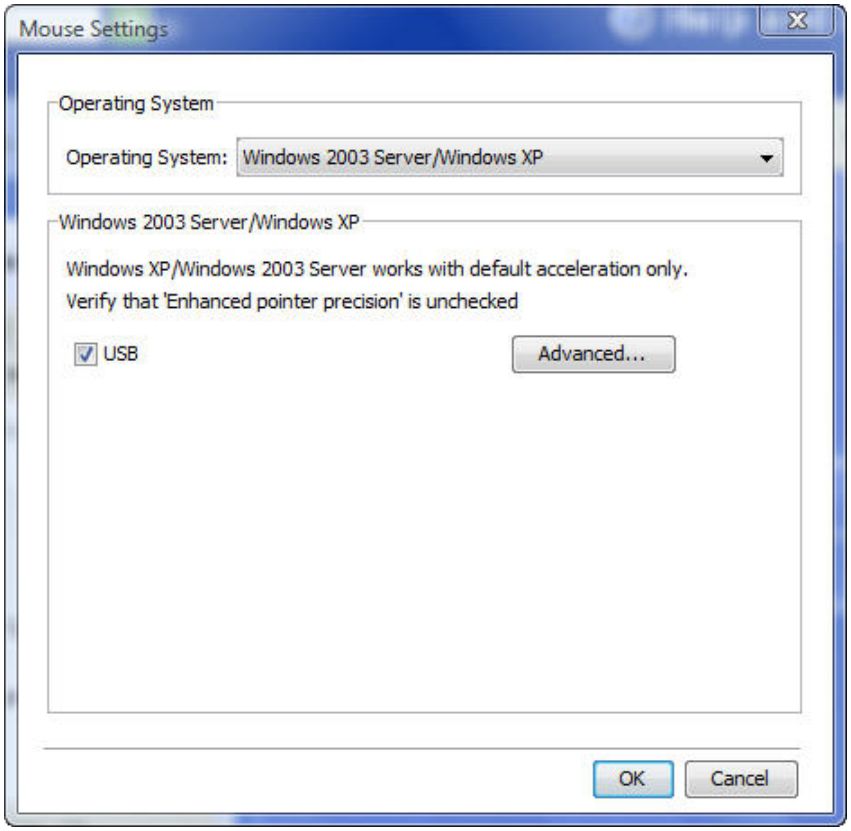


Figure 42 – Relative Mouse Settings

2. In **Operating System**, from the dropdown menu, select the target's operating system.

   Instructions and sliders appear.

3. Follow the instructions and set any relevant sliders to the same values as set in the target's Mouse Properties window.
4. Click **OK**.

   The mouse pointers are synchronized.

Examples

The following are examples of the instructions for two different target operating systems. After performing the instructions for the selected operating system, you should click **OK** to synchronize the mouse pointers.

1. For **Windows 7**: Go to the Mouse Properties on the Target and clear the **Enhance pointer precision** checkbox.

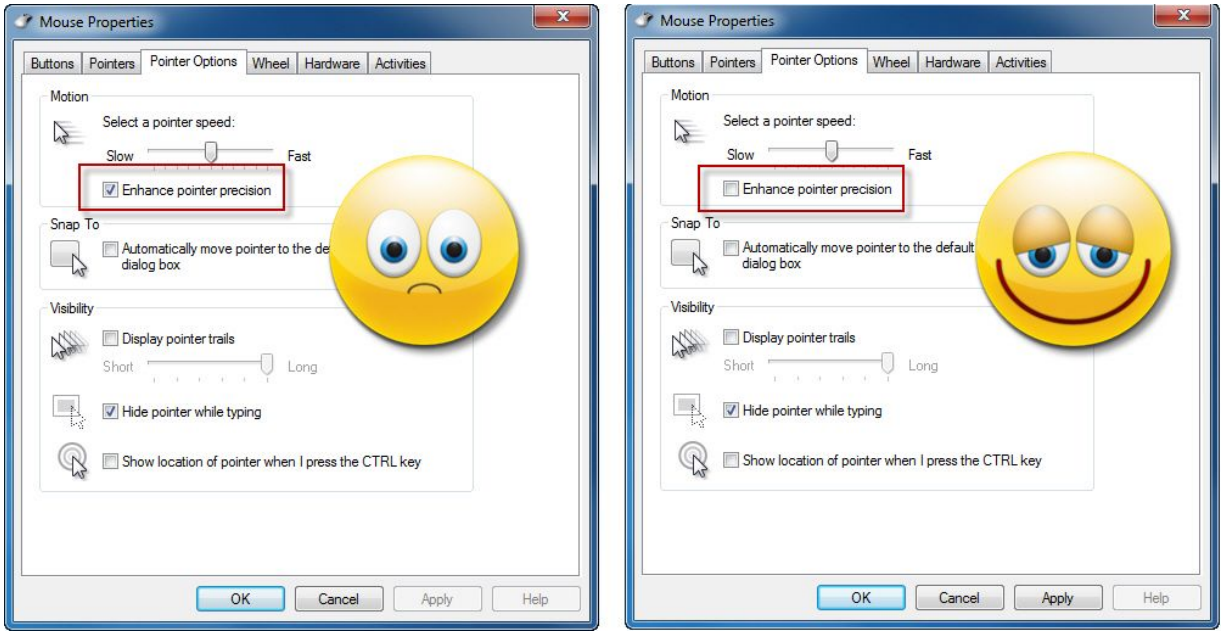


Figure 43 – Windows 7 Mouse Properties

2. For **Windows 2000**: If Mouse Properties were ever changed for the target – even if they have been returned to their original state – clear the **Default** checkbox

   ☑ Default

The USB Option

You can use the **USB** option if you have USB to PS2 conversion between Smart 108/116 IP and the target server via any of the following:

- USB-to-PS/2 adapter
- USB KVM dongle, such as RICC/ROC USB and X-RICC USB
- Unsupported operating systems
- SUN Solaris

Use this option if you are sure of the custom acceleration algorithm you are using, or have been informed to do so by customer support.

Advanced Mouse Emulation

In the Advanced Mouse settings, you can set the type of mouse that you would like Smart 108/116 IP to emulate. It is recommended not to change the advanced settings unless there is erratic mouse behavior (for example, the mouse is making random clicks and jumping arbitrarily around the screen).

These settings come into effect when Smart 108/116 resets the local mouse after the KVMIP session is over.

➔ **To set the type of mouse that you want Smart 108/116 IP to emulate:**

1. In the **Mouse Settings box** (see Figure 42), click **Advanced**.

   The Mouse Emulation box appears.

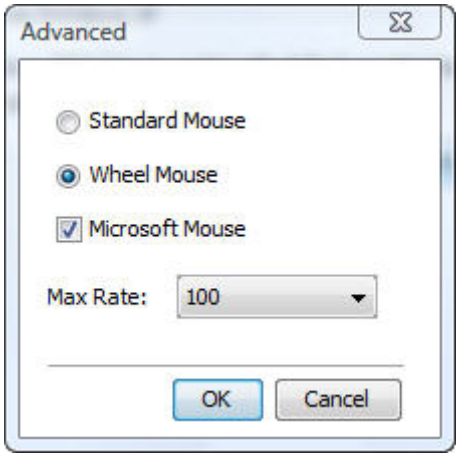


Figure 44 – Mouse Emulation Box

2. Select the mouse connected to the Local Console port on the Smart 108/116 IP, as follows:
   - **Standard Mouse** – if the local mouse is a non-Microsoft two-button mouse; in this case, clear the **Microsoft Mouse** checkbox.
   - **Wheel Mouse** – Microsoft mouse or Microsoft optical mouse

3. In **Max Rate**, select the maximum mouse report rate.

   For Sun Solaris the default value is 20 in order to support older Sun versions.

4. Click **OK**.

4.9.2 Aligning the Mouse Pointers

When accessing the target server, the mouse pointers may appear at a distance to each other, due to the mouse on Smart 108/116 IP losing sync with the mouse on the host system. You can align the local mouse pointer with the remote target device's mouse pointer.

➔ **To align the mouse pointers:**

1. On the toolbar, select  **> Align** (or press **Ctrl+M**).

   The mouse pointers align.

4.9.3 Calibrating Mouse Pointers

A target server may have a different mouse pointer speed than the client computer. Calibrating automatically discovers the mouse speed of the target server and aligns the two pointers.

You can perform automatic calibration when the target server operating system is Windows NT4, 2000, or 98.

Smart 108/116 IP saves this alignment so that calibration is only needed once per target server.

➔ **To perform the calibration:**

1. On the toolbar, select  **> Calibrate**.

If the Video Noise Level is above zero, calibration may not work. In this case, go to Video Adjustment and try to eliminate the noise by automatically adjusting the video (see Section 4.7.2) and/or adjusting the bars in manual video adjust (see Section 4.7.3), and then performing the mouse calibration.

If the mouse settings on the target server have been changed, you must synchronize mouse pointers manually, as explained below.

4.10 Switching to a Different Server

In the middle of a remote session, you can switch to a different server.

➔ **To connect to a different server:**

1. On the toolbar, click  .

   A list of connected servers appears. There is a checkmark near the server of the remote session.

2. Click the desired server.

   The screen of the server terminal emulation window appears.

4.11 Disconnecting the Remote Session

➔ **To disconnect the session:**

1. On the toolbar, click  .

   The Login Web page appears. You can re-login or close the browser window.

5 Troubleshooting – Safe Mode

From Safe mode, you can:

- **Restore factory defaults** – When you cannot access the system (for example, you have forgotten the Username or Password), you can restore factory defaults from Safe mode (see Section 3.8.3 on page 40 on how to restore factory settings from the Web interface).
- **Restore the device firmware** – If during a firmware update there is a power failure and you can no longer access the system, you can restore the device firmware from Safe mode, using a special update file.

5.1 Entering Safe Mode

The following flowchart provides an overview on how to enter Safe mode.

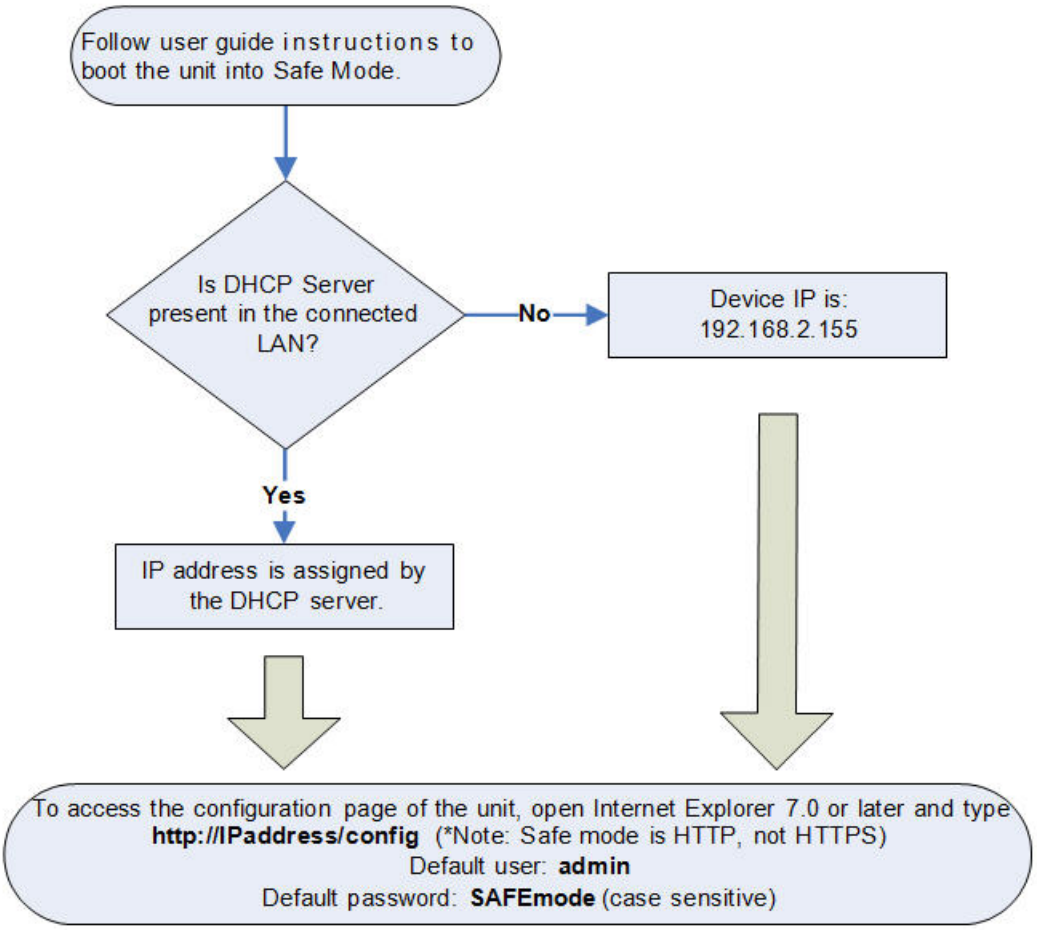


Figure 45 – Safe Mode Procedure

➔ **To enter Safe mode:**

1. While powering up Smart 108/116 IP, press and hold down the **Go Local** button on the back panel of the unit for three to four seconds.

   The device boots up in Safe mode.

2. Wait until the unit finishes booting (one to two minutes).
3. Determine the IP address of the Smart 108/116 IP unit. The IP address depends on whether or not there is a DHCP server on the network. If there is, the DHCP server assigns an IP address to the Smart 108/116 IP unit. If there is no DHCP server, the unit boots with the static IP address 192.168.2.155.
4. Open Internet Explorer and type into the Address box: http://IP address/config. (Do not start the address with **https**.)

   The Login page appears.

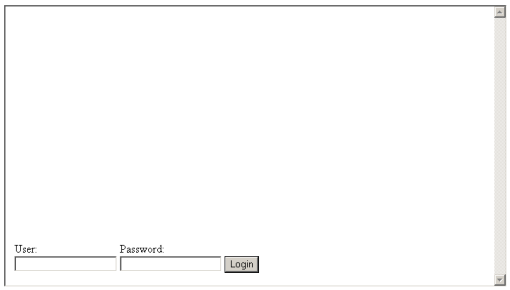


Figure 46 – Login Page

5. In **User**, type username **admin** , and in **Password**, type **SAFEmode** (case sensitive). (This username and password works only in Safe mode.)

   A menu appears.

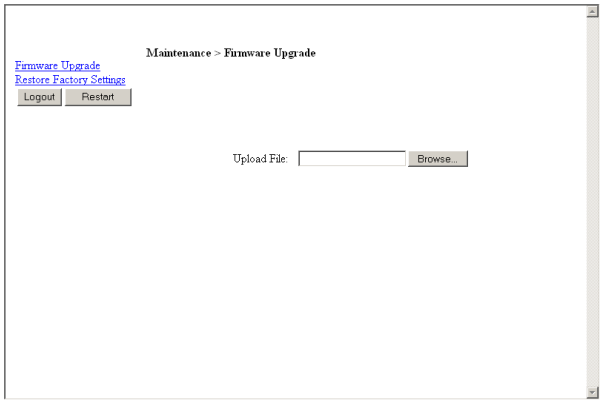


Figure 47 – Safe Mode Menu

5.2 Restoring Factory Defaults

You can restore all Smart 108/116 IP settings to their default values.

➔ **To restore factory defaults:**

1. In the Safe Mode menu (see Figure 47), click **Restore Factory Settings**.

   A warning appears.

Figure 48 – Warning

2. Click Restore.

   An additional warning appears.

Figure 49 – Additional Warning

3. Click **OK**.

   The factory defaults are restored. When the process finishes, the following figure appears.

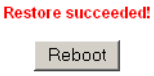


Figure 50 – Reboot

4. Click **Reboot** to restart the unit.

5.3 Restoring the Device Firmware

To receive the Upgrade firmware required to restore the device firmware, contact Minicom Technical Support support@minicom.com. Save the Upgrade firmware on the hard disk of a computer connected to the network.

➔ **To restore device firmware:**

1. In the Safe Mode menu (see Figure 47), click **Firmware Upgrade**.

   A warning appears.

2. Locate the Upgrade firmware, click **Install**, then click **Start Upgrade**.

   The firmware upgrades. When the process finishes, the following figure appears.

Figure 51 – Upgrade Succeeded

3. Click **Reboot** to restart the unit.

6 Operating the Smart 108/116 IP Switching System Locally

This chapter explains how to operate the Smart 108/116 IP Switching system locally, as well as how to upgrade the Smart 108/116 IP firmware (see Section 6.3) and troubleshoot problems that arise when updating the software (see Section 6.4).

You can switch between the connected computers using either the:

- Keyboard hotkeys
- The OSD (On Screen Display)

With a US English keyboard, you can use the **+** key of the alphanumeric section or of the numeric keypad. With a non-US English keyboard, only use the **+** key of the numeric keypad.

6.1 Using the Keyboard Hotkeys

You can switch to the next computer in the forwards or backwards direction.

➔ **To switch to the next computer forwards:**

1. Press **Shift.**
2. Release **Shift** and then press **+**.

➔ **To switch to the next computer backwards:**

1. Press **Shift.**
2. Release **Shift** and then press **-**.

6.2 Using the OSD

➔ **To display the OSD:**

1. Ensure that there is no remote user connected.

   If there is a remote user, disconnect the remote user by pressing the **Local** button on the Smart 108/116 IP.

2. Press **Shift** twice.

   The OSD Main window appears.

Figure 52 – OSD Main Window

Lines with yellow text show active computers. Lines with blue text show inactive computers. The **Type** column indicates that a computer "C" is connected to the port.

6.2.1 Navigating the OSD

You can navigate the OSD, as follows:

- To move up and down – Use the **Up** and **Down** arrow keys.
- To jump from one column to the next (when relevant) – Use the **Tab** key.
- To exit the OSD or return to a previous window within the OSD – Press **Esc.**

6.2.2 Selecting a Computer

➔ **To select a computer:**

1. Navigate to the desired computer line.

   OR

   Type the port number of the desired computer.

2. Press **Enter**.

   The selected computer is accessed. A Confirmation label appears showing which computer is accessed.

When the OSD is displayed, you cannot select computers using the keyboard hotkeys.

6.2.3 Configuring the OSD Settings

You can configure the following OSD settings:

- General (see Section 6.2.4)
- Ports (see Section 6.2.5)
- Time (see Section 6.2.6)
- Users (see Section 6.2.7)
- Security (see Section 6.2.8)

You can also view the available Help (see Section 6.2.9).

➔ **To configure the OSD settings:**

1. Press **F2**.

   The OSD Settings window appears.

Figure 53 – OSD Settings Window

When the OSD is password protected (explained below), only the Administrator has access to the F2 settings window.

6.2.4 Configuring the General Settings

From the General Settings screen, you can configure the following general settings:

- Security
- OSD hotkey
- Autoskip

- Keyboard language
- Switch name

From this screen, you can also restore the OSD to its factory default.

➔ **To configure the general settings:**

1. In the OSD Settings window (see Figure 53), navigate to **GENERAL** so that the red line is on it, and press **Enter**.

   The General Settings window appears.

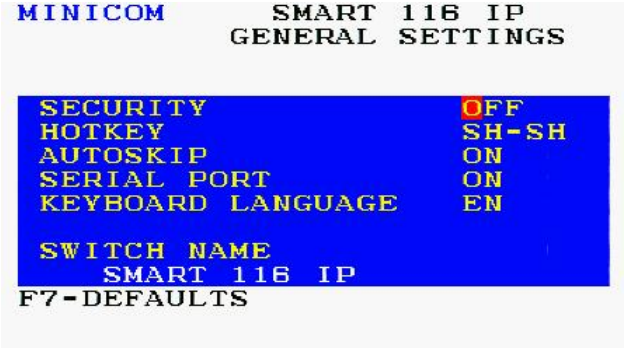


Figure 54 – General Settings Window

Configuring Security Settings

The OSD comes with an advanced password security system that contains three different security levels. Each security level has different access rights to the system, as follows:

- **Administrator (Status A)** who can:
  - Set and modify all passwords and security profiles
  - Fully access any computer
  - Use all OSD functions
- **Supervisor (Status S)** who can:
  - Fully access any computer
  - Access the following OSD functions only – F4 Scan, F5 Tune, and F6 Moving the Confirmation label.
- **User (Status U)** – There are six different Users in the Smart 108/116 IP system. Each User has a Profile set by the Administrator that defines the access level to

different computers. There are three different access levels – explained in Section 6.2.7 on page 74.

Activating Password Protection

By default, OSD access is not password protected. Only the Administrator can password-protect the OSD or disable password protection.

➔ **To activate password protection:**

1. In the General settings window (see Figure 54), navigate to the **Security** line.
2. Press the Space bar to toggle between **Security On** and **Off**.

   The password dialog box appears.
3. Type the Administrator's password (default is "admin").
4. Press **Enter**.

   The new security status is set.

Changing the OSD Hotkey

By default, pressing **Shift, Shift** displays the OSD.

You can replace the OSD hotkey **Shift, Shift** with any of the following:

- **Ctrl, Ctrl**
- **Ctrl, F11**
- **Print Screen**

➔ **To change the hotkey:**

1. In the General settings window (see Figure 54), navigate to the **Hotkey** line.
2. Press the Space bar to toggle between the available options.

   From now on, you can press this new hotkey to display the OSD.

Activating Autoskip

With the Autoskip feature, the arrow keys only access the active computer lines on the OSD. When **Autoskip** is **Off**, the arrow keys access both active and inactive computer lines.

➔ **To change the Autoskip setting:**

1. In the General settings window (see Figure 54), navigate to the **Autoskip** line.
2. Press the Space bar to toggle between Autoskip **On** and **Off**.

Serial Port

This option is disabled in Smart 108/116 IP. Leave this option on its default setting **ON**.

Changing the Keyboard Language

The keyboard language is preset to US English. You can change the keyboard language to French (FR) or German (DE).

➔ **To change the keyboard language:**

1. In the General settings window (see Figure 54), navigate to the **Keyboard Language** line.
2. Press the Space bar to toggle between the available options.

Editing the Switch Name

The Switch name is displayed under **Switch Name** in the General settings window (see Figure 54). You can substitute up to 18 characters in the line; a space is considered a character. When there is more than one switch in the system, give each Switch's OSD a different name.

Restoring OSD to Factory Defaults (F7)

In the General settings window (see Figure 54), you can press F7 to restore the OSD to its factory default settings.

Restoring factory default settings erases all changes that have previously been made.

6.2.5 Configuring the Ports Settings

From the Ports settings window, you can configure the following:

- The Computer name
- The Keyboard settings

➔ **To configure the ports settings:**

1. In the OSD Settings window (see Figure 53), navigate to **PORTS** so that the red line is on it, and press **Enter**.

   The Ports Settings window appears.

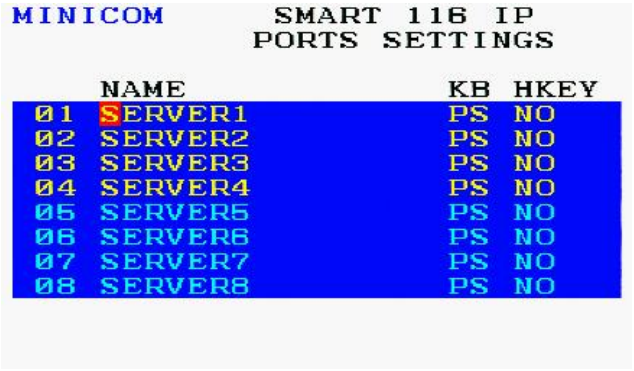


Figure 55 – Ports Settings Window

Editing the Computer Name

In the Ports Settings window, the computer names can be up to 15 characters long.

To avoid confusion, the names given in the OSD should match the names given in the Web configuration.

➔ **To edit a computer name:**

1. In the Ports Settings window (see Figure 55), navigate to the **Name** column, to the name that you want to edit.
2. Edit the name, as follows:
   - To erase a character – Select it and press the Space bar. A blank space replaces the erased character.
   - To erase an entire line – Place the cursor at the beginning of the line, and keep the Space bar depressed until the line is erased.

Modifying the Keyboard Setting

The Smart 108/116 IP operates with Windows, Linux, HP UX, Alpha UNIX SGI, DOS, Novell, MAC-USB, or Open VMS.

By default, the keyboard mode is set to PS, which is suitable for Intel-based computers and UNIX servers connected to ROC/RICCs USB.

For systems with UNIX servers connected to ROC/RICCs PS/2, set the KB column as follows:

- **U1** for HP UX
- **U2** for Alpha UNIX, SGI, and Open VMS

- **U3** for IBM AIX

➔ **To modify the keyboard settings:**

1. In the Ports Settings window (see Figure 55), navigate to the **KB** column, and go to the line that you want to edit.
2. Press the Space bar to toggle between the available options.

6.2.6 Configuring the Time Settings

➔ **To configure the time settings:**

1. In the OSD Settings window (see Figure 53), navigate to **TIME** so that the red line is on it, and press **Enter**.

   The Time Settings window appears.

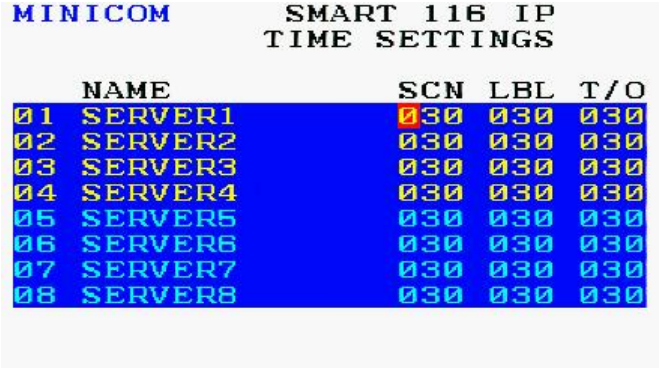


Figure 56 – Time Settings Window

Setting the Scan, Label, and Timeout Period

In the Time Settings window, you can set the following:

- **SCN** – the scan period
- **LBL** – the display period of the Confirmation label, showing which computer is currently accessed
- **T/O** – the timeout period. When password protection is activated, you can automatically disable the Management keyboard, mouse, and screen after a preset time of nonuse.

➔ **To set the above periods:**

1. Navigate to the desired column and row.
2. Place the cursor over one of the three digits and type a new number for the new time period. Type a leading zero where necessary. For example, type **040** for 40 seconds. The numbers **000** and **999** are reserved, as follows:

- In the **LBL** column – Typing **999** displays the label continuously; typing **000** hides the label.
- In the **T/O** column – Typing **999** disables the Timeout function. Typing **000** causes the Timeout function to work immediately.
- In the **SCN** column – Typing **999** displays the screen for 999 seconds. Typing **000** causes the computer screen to be skipped.

6.2.7 Configuring the Users Settings

➔ **To configure the users settings:**

1. In the OSD Settings window (see Figure 53), navigate to **USERS** so that the red line is on it, and press **Enter**.

   The Users Settings window appears.

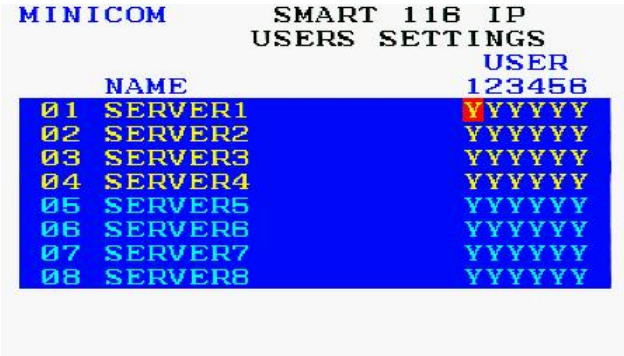


Figure 57 – Users Settings Window

Users is only enabled if the security status is set to On (see the Configuring Security Settings section on page 69).

There are three different access levels:

- **Y** – Full access to a particular computer.
- **V** – Viewing access only to a particular computer (no keyboard/mouse functionality).
- **N** – No access to a particular computer; a TIMEOUT label appears if access is attempted.

➔ **To give each user the desired access level:**

1. In the Users Settings window, navigate to the desired computer line and **User** column.

2. Toggle between the options using the **Space** bar.

6.2.8 Configuring the Security Settings

➔ **To configure the security settings:**

1. In the OSD Settings window (see Figure 53), navigate to **SECURITY** so that the red line is on it, and press **Enter**.

   The Security Settings window appears.

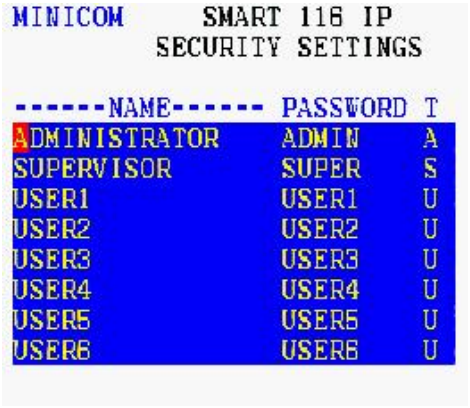


Figure 58 – Security Settings Window

Security is only enabled if the security status is set to On (see the Configuring Security Settings section on page 69).

The **T** column in the Security Settings window displays the **Type** of access permission. In this column, there can be one Administrator (**A**) password, one Supervisor (**S**) password, and six User (**U**) passwords.

➔ **To change a user name or password:**

1. In the Security Settings window, navigate to the desired row and column.
2. Type a new user name and/or password. User authentication is done solely via the password; there is no security significance to the name.

By default, the User Profile settings are full access.

6.2.9 OSD Functions (F1)

The OSD has functions that you can activate from the main window. These functions include:

- Scan (F4)

- Tune (F5)
- Move Label (F6)
- New Monitor - DDC2 (F10)

You can view the available functions from the OSD Help window.

➔ **To view the available OSD functions:**

1. In the General settings window (see Figure 54), press **F1**.

   The Help window appears. It displays the functions that can be performed from the main window (see Figure 52).

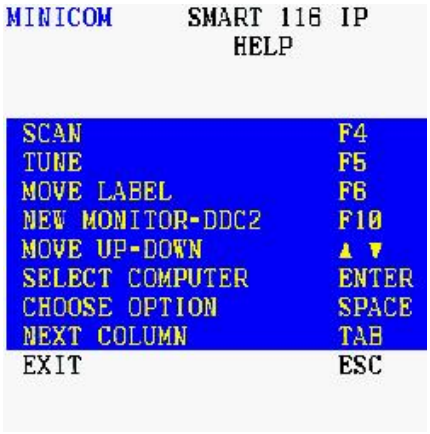


Figure 59 – The OSD HELP Window

All the functions listed in the Help window can be performed from the Main window. The Help window is merely a reminder of the hotkeys and their functions.

Scanning Computers (F4)

When necessary, you can adjust the scan time in the Time Settings window (Figure 56).

➔ **To activate scanning:**

1. Press **Shift** twice to open the OSD.
2. Press **F4**.

   Your screen displays each active computer sequentially, with the Scan label appearing in the top left corner.

➔ **To deactivate scanning:**

1. Press **F4**.

Tuning (F5)

You can tune the image of any computer screen from the Select Computer window, accessed from the Main window (see Section 6.2.2).

➔ **To adjust the screen image:**

1. Navigate to the computer that you want to adjust.
2. Press **F5**.

   The screen image of the selected computer appears, together with the Image Tuning label.

3. Use the **Right** and **Left** arrow keys to adjust the image.
4. When the image is satisfactory, press **Esc**.

Picture quality is relative to distance. The further away a remote computer is from the Smart 108/116 IP, the lower the image quality, and the more tuning is required. Therefore, place the higher resolution computers closer to the Switch.

Moving the Label (F6)

You can position the Confirmation label anywhere on the screen.

➔ **To position the label:**

1. In the main window (see Figure 52), navigate to the desired computer using the **Up** and **Down** arrow keys.
2. Press F6.

   The selected screen image and Confirmation label appear.

3. Use the arrow keys to move the label to the desired position.
4. Press **Esc** to save and exit.

Inputting and Updating DDC Information (F10)

Display Data Channel (DDC) is a VESA standard for communication between a monitor and a video adapter.

When first installing the system, input the DDC information of the monitor connected to the Smart 108/116 IP switch into the memories of all connected ROC/RICCs.

➔ **To input the DDC information:**

1. Disconnect the Video cable of all RICCs from the computers. ROCs do not need to be disconnected.
2. Press **Shift** twice to open the OSD.
3. Press **F10**.

   "Please wait" flashes a few times and disappears. The monitor's DDC information is sent to all ROC/RICCs.
4. Reconnect the Video cable of all RICCs.

You should update the DDC information in any of the following circumstances:

- When replacing the monitor connected to Smart 108/116 IP Switch
- When adding a new ROC/RICC to the system
- When reconnecting an existing ROC/RICC that was temporarily used in a different system

To update the DDC information, follow the steps in the procedure for inputting DCC information.

6.3 Upgrading the Smart 108/116 IP Firmware

With the Smart 108/116 IP Switch Update software, you can upgrade the firmware for the:

- Switch processors
- RICC/ROCs

The Update software enables you to add new features and fix bugs in a quick and efficient manner. You can also return the OSD to the factory default settings via the Update software. You can install the Update software on any computer, even one that is not part of the Smart 108/116 IP system.

6.3.1 Downloading Update Software and Latest Firmware

The Update software and latest firmware for your system are located on our website at: http://www.minicom.com/phandlc.htm

You can download any of the following firmware packages:

- Complete Firmware Package – This includes the firmware for all Smart switches and RICCS and ROCS.

- Firmware Package for Smart Switch models – This includes the firmware for all Smart switches.
- Smart CAT5 Switch Firmware – There are multiple hardware versions of Smart CAT5 Switch units, each with version specific firmware. On the Web page, find the description and table that identifies your version.
- Firmware Package for RICC and ROC models – Download a firmware package for RICC and ROC models (see the table on the Web page for the supported RICC/ROC models). Or, search for and download the specific RICC/ROC models with the correct firmware version.

6.3.2 Update Software System Requirements

The following are the Update software system requirements:

- Pentium II class computer with 256 MB RAM and 10 MB free hard drive space
- Free Serial port
- Windows 2000 or later

6.3.3 Connecting the Smart 108/116 IP System

To update the firmware, the Smart 108/116 IP system must be connected and switched on.

6.3.4 Connecting the RS232 Download Cable

To run the Update software, you must connect the RS232 Download cable (p/n 5CB40419) to the computer containing the software, and to the Smart 108/116 IP Switch Flash port.

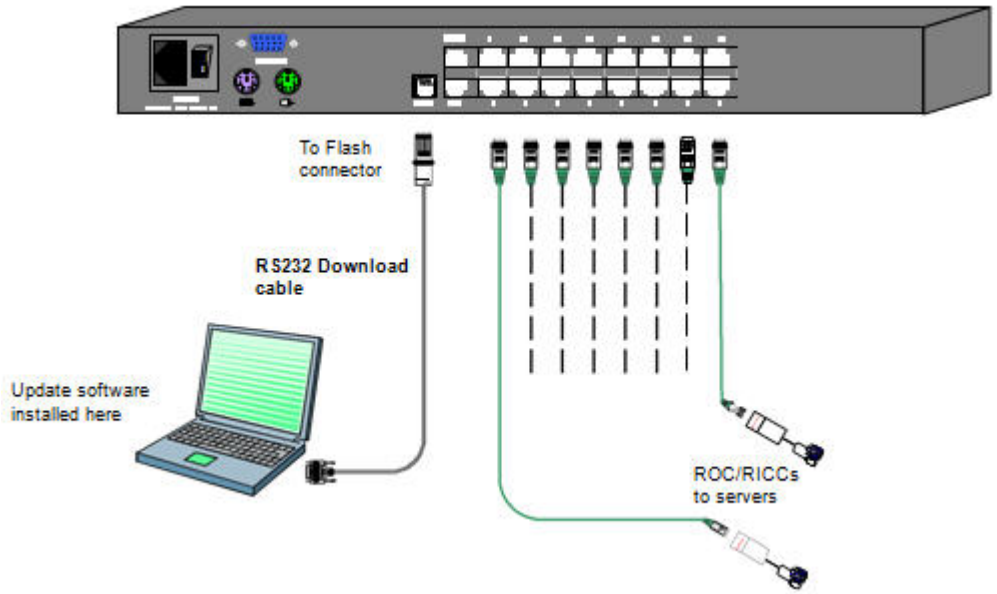


Figure 60 – RS232 Cable

6.3.5 Installing the Software

➔ **To install the Update software:**

1. Download the software from the Support section of Minicom's website.
2. Install the software on the computer's hard drive.

6.3.6 Starting and Configuring the Update Software

➔ **To start and configure the Update software:**

1. Select **Start/Programs/Smart IP Switch Update/Smart IP Switch Update** or click the shortcut icon on the Desktop 

.

   The Smart IP Switch Update window appears.

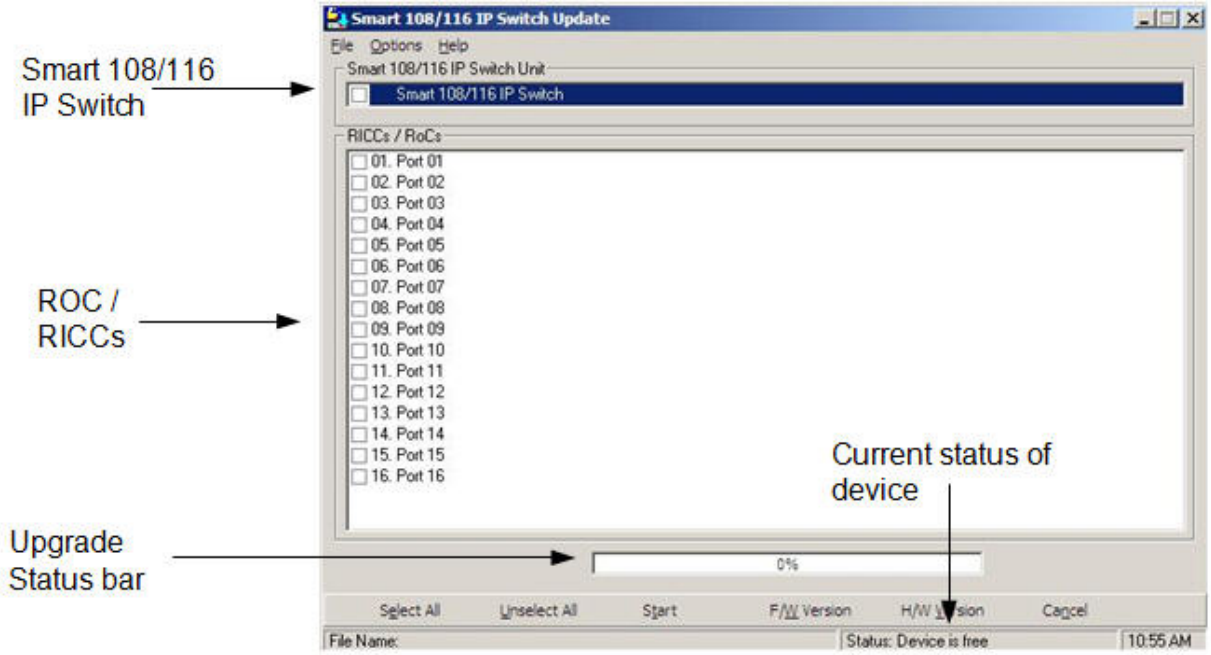


Figure 61 – Smart 108/116 IP Switch Update Window

The table below explains the functions of the buttons and dialog boxes in the Update window.

Button/Box	Function
Select All	Selects all RICC/ROCs
Unselect All	Unselects selected RICC/ROCs
Start	Starts the firmware download
F/W Version	Displays the firmware version numbers
H/W Version	Displays the hardware version numbers
Cancel	Cancels the selected function
10:06	System time
Status:	Displays the communication status between the upgrade software and the Smart 108/116 IP. Choose **Options/Get Status** to refresh the status.
File Name:	Name of Update file

2. Install the software on the computer's hard drive.
3. To change the Com Port from the Options menu, choose **Com Port**.

   The Communication Port Dialog box appears.

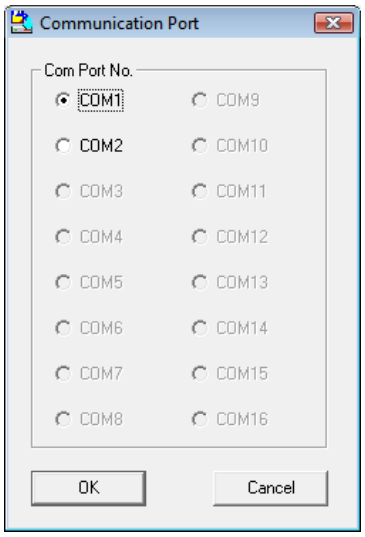


Figure 62 – Communication Port Dialog box

4. Choose the Com Port that the RS232 Serial cable is connected to, and click **OK**.

6.3.7 Verifying the Version Numbers

Before upgrading the firmware, you must verify which firmware and hardware versions you have.

Smart 108/116 IP Switch Version

➔ **To verify the Smart 108/116 IP Switch version:**

1. Select the **108/116 IP Switch** checkbox.
2. Click F/W Version.

   The firmware versions of the Translator, Master, and OSD appear.

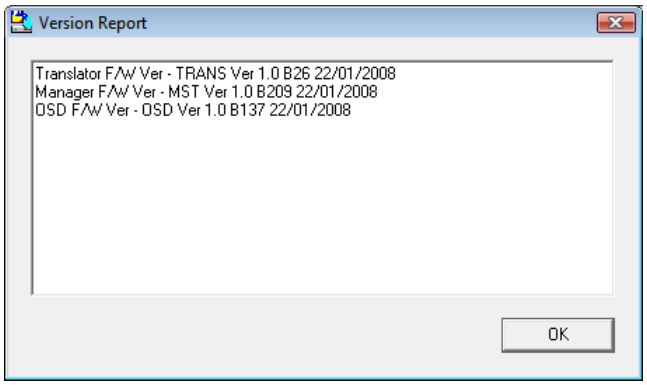


Figure 63 – Firmware Version Report

3. Click H/W Version.

   The hardware version of the Translator appears.

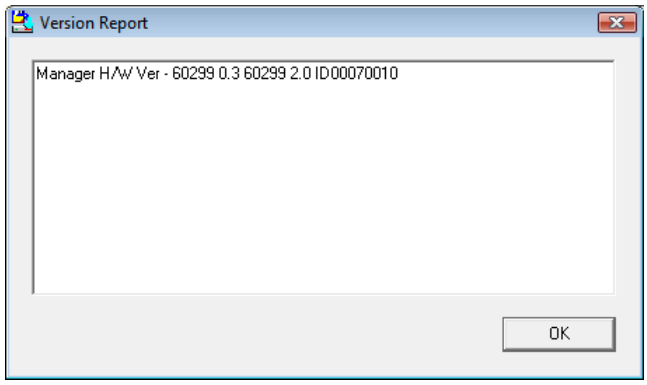


Figure 64 – Hardware Version Report

RICC/ROC Version

Before you can select a RICC/ROC, you must clear the **108/116 IP Switch** checkbox.

➔ **To verify the RICC/ROC version number:**

1. Select one or more or all of the RICC/ROCs.
2. Click F/W Version.

   The firmware version number appears.
3. Click H/W Version.

   The hardware version number appears.

   When "Not responding" appears, it indicates that no computer is connected, or that it is switched off.

6.3.8 Obtaining New Firmware

Download the latest firmware for your system from www.minicom.com.

Updating the Firmware

During the Update process, do not switch off any computer connected to the Smart 108/116 IP system.

➔ **To update the firmware:**

1. Select the option to update the Smart 108/116 IP switch or the RICC/ROCs.
2. From the File menu, choose **Open**.

   The Open dialog box appears.

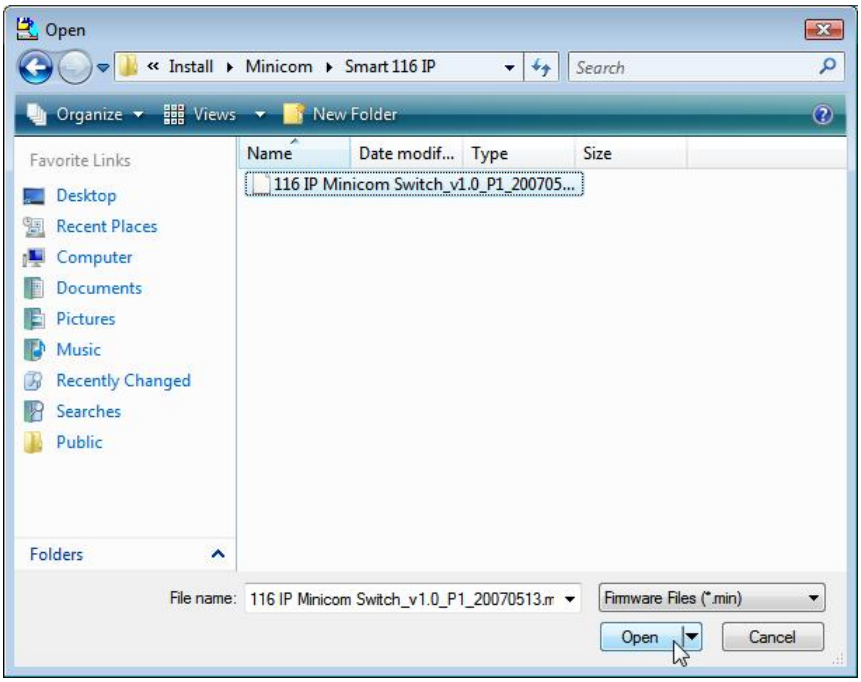


Figure 65 – Open Dialog Box

   The Smart 108/116 IP switch update is a .min file. The RICC/ROC update is a .hex file.

3. Navigate to the folder that contains the firmware update file. You can only see the files that match the file selection mask. When the firmware is contained in a Firmware Package, select the package. The package comes with a .min extension. The correct firmware is automatically selected according the Switch or RICC/ROCC chosen in step 1 above. The file extension for specific devices is .hex.
4. Open the file.
5. Click **Start**.

   The Smart 108/116 IP Switch Update flashes the firmware. On completion, the firmware version number appears.

If the status of the device is busy - see the bottom of Figure 61- the system cannot be upgraded. To free the device, choose **Options/Advanced/Reset**. The device resets and the status is now free. Click **Start**.

6. Check that the updated version number is correct by pressing F/W Version.

Manually Updating the RICC/ROCs

You can manually update the RICC/ROCs after starting the Update software.

➔ **To manually update the RICC/ROCs:**

1. Select one or more ROCs..
2. Press **Options -> Advanced -> Manual Update**.
3. Open the appropriate hex file.
4. Click **Start**.

   The firmware updates.

6.3.9 Restoring Factory Settings

You can restore the OSD to the factory settings from the Update software.

All changes made (such as passwords, access rights, and names) will be removed.

➔ **To restore the OSD factory settings:**

1. Select **Options/Advanced/Set default**.

   The OSD returns to the factory default settings.

You can also restore the OSD default settings from the OSD (F7) (see page 71)

6.4 Troubleshooting – Update Software

This section describes how to troubleshoot the following two problems that may arise when updating the Smart 108/116 IP firmware:

- Communication Error message
- Electricity failure

6.4.1 Communication Error Message

When updating a unit, a Communication Error message may appear.

➔ **To fix the communication problem:**

1. Check that the RS232 Serial cable's RS232 connector is connected to the switch's Flash port.
2. Check that the RS232 Serial cable's DB9F connector is connected to the laptop's Serial port.
3. Verify that there is no Remote session in progress by pressing the **Local** button.
4. Restart the update process.

6.4.2 Electricity Failure

The electricity may fail while updating the Smart 108/116 IP firmware.

- If the electricity fails during the firmware update of the switch, a Communication Error message appears. Simply resume the firmware update by opening the folder that contains the firmware update file and continue from there.

- If the electricity fails during the firmware update of the RICCs, a Not Responding or Upgrade Error message appears. Restart the upgrade from the beginning.

- For an electricity failure during a firmware upgrade of the digital part of the Smart108/116 IP, enter the device Safe mode and restore the device to its default settings.

7 Technical Specifications

Specification	Description
Operating systems	**Target server** – DOS, Windows, Novell, Linux, or SUN Solaris for PC **Client computer** – Windows 2000 or later with Internet Explorer 7.0 / Firefox 3.0 and later; Linux x86 with Firefox 3.0 and later
Resolution	**Target server** – Up to 1600 x 1200 @ 85 Hz **Client computer** – Recommended resolution should be higher than on target server
Video and mouse synchronization	Both auto and manual modes
Security	SSL, high grade 256-bit AES encryption
Connections	**Ethernet** – RJ45 – 10/100 Mbit/sec autosensing **Serial** – RJ45 **Local KVM connection** – Screen HDD15; Keyboard/Mouse – MiniDIN6 **Flash** – RJ11 **Server** – RJ45
Weight	2.54 Kg / 5.6 lb
Dimensions (H x D x W)	44 x 220 x 431 mm / 1.6 x 8.66 x 17 in
Power input	100-240 VAC, 0.8 A, 50/60 Hz
Operating temperature	0°C to 40°C / 32° to 104°F
Storage temperature	-40°C to 70°C / -40°F to 158°F
Humidity	80% non-condensing relative humidity

Specification	ROC PS/2	ROC USB
Connections	**VGA** – HDD15 **KM** – MiniDin6 **System** – RJ45	**VGA** – HDD15 **KM** – USB **System** - RJ45
Power	From Keyboard port	From USB port
Product Weight	100 g / 0.20 lb	

Specification	ROC PS/2	ROC USB
Shipping Weight	172 g / 0.38 lb	
Dimensions (H x D x W)	65 x 25 x 25 mm / 2.55 x 0.98 x 0.98 in	

8 Video Resolution and Refresh Rates

Hz →	56	60	65	66	70	72	73	75	76	85	86
640x480		x		x	x	x		x		x	
720x400					x					x	
800x600	x	x				x		x		x	x
1024x768		x			x	x	x	x	x	x	
1152x864								x			
1152x900				x					x		
1280x720		x									
1280x768		x						x			
1280x960		x								x	
1280x1024		x				x		x	x	x	
1600x1200		x	x		x			x		x	

9 SNMP Events Table

The following table lists all recorded events.

Event Text	Code	Comment
System Boot	1010	Reported upon device boot-up.
Server Busy ask for disconnect.	1030	Attempt to connect when another user is already connected. The second user has permission for takeover; sent before the second user actually takes over the session.
User login succeeded	1040	On every successful user login to the device.
Login failed wrong user name or password	1050	Login failed due to wrong user name or password.
Login not succeeded server busy	1060	Login denied because a user with higher permission is connected (takeover not allowed).
Logout	1070	User Logout (end of remote access session).
Disconnected by another user	1110	Takeover has been successfully performed; the previous user has been disconnected.
Hardware Failure	1200	Device internal hardware failure. Try disconnecting any other attached device and reboot. If problem persists, contact technical support.
Hard reset power cycle command	1220	Power cycle command issued; only relevant when a special power-cycle product is attached to the device (for exmple, KBPower).
Viewer login	1230	User connected in view-only mode (while another user is connected in a regular session).
Viewer logout	1240	User connected in view-only mode has disconnected.
Global access disabled	1250	Device has been blocked for access by an administrator; remote access is disabled until the device is unblocked.
Block User Account	1260	User blocked due to too many login attempts; failure per policy in configuration.
Successful User Login	2010	Successful User Login. CONF_USER_EVENT_LOGIN_SUCCEEDED
Login is not successful – wrong user access level.	2020	Login is not successful – wrong user access level. CONF_USER_EVENT_LOGIN_NOT_SUCCEEDED_WRONG_LEVEL

Event Text	Code	Comment
Wrong user name or password	2030	Wrong user name or password. Login is not successful. CONF_USER_EVENT_LOGIN_NOT_SUCCEEDED_WRONG_USER_NAME_OR_PASSWOR D
Login is not successful because server is busy.	2040	Login is not successful because server is busy. CONF_USER_EVENT_LOGIN_NOT_SUCCEEDED_SERVER_BUSY
DHCP server setting has been changed	2060	DHCP server setting has been changed. CONF_DHCP_CHANGED
Network IP address changed	2070	Network IP address has been changed. CONF_IP_CHANGED
Network Subnet Mask changed	2080	Network Subnet Mask has been changed. CONF_SNMASK_CHANGED
Network Default Gateway changed	2090	Network Default Gateway has been changed. CONF_DG_CHANGED
User Logged out from Config	2100	User Logged out from Config. CONF_LOG_OUT
TCP Port was changed	2110	TCP Port was changed. CONF_TCP_PORT_CHANGED
Remote Access type was changed	2120	Remote Access type was changed. CONF_REMOTE_ACCESS_CHANGED
Security settings changed	2140	CONF_SECURITY_CHANGED
Restore default factory settings successful	2150	CONF_RESTORE_FACTORY_OK
Restore default factory settings failed	2160	CONF_RESTORE_FACTORY_FAILED
Firmware Upgrade successful	2170	CONF_UPGRADE_OK
Firmware Upgrade failed	2180	CONF_UPGRADE_FAILED


MINICOM
advanced systems